SUCELLOS

Public security target

IAS ECC v2 on ID-One Cosmo V7.1-s Card (Standard Dual and Basic Dual)

WWW.OBERTHUR.COM

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com

S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

DOCUMENT REVISION HISTORY		
Issue	**Date**	**Purpose**
1	08/12/2013	Creation of the document

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

TABLE OF CONTENTS

1 INTRODUCTION 6

1.1 SECURITY TARGET REFERENCE 6
1.2 REFERENCES 6
1.3 DEFINITIONS 8

2 TARGET OF EVALUATION 10

2.1 OVERVIEW 10
2.1.1 TOE Type 10
2.1.2 Logical scope 10
2.1.3 Physical scope 12
2.1.4 Required non-TOE hardware/software/firmware 14
2.1.5 Usage and major security features 14
2.1.6 Scope of evaluation 15
2.2 DESCRIPTION 15
2.2.1 Data structure 16
2.2.1.1 File and File System 16
2.2.1.2 Security Environment 18
2.2.1.3 Security data Objects 19
2.2.2 Access Control Management 20
2.2.3 Authentication of entities 21
2.2.4 Electronic Services 21
2.2.5 Administration of the TOE 21
2.2.6 Single Sign on feature (SSO) 21
2.3 REFERENCE 22
2.4 LIFE CYCLE 24
2.4.1 Development 25
2.4.1.1 Software development (phase 1) 25
2.4.1.2 Hardware development (Phase 2) 25
2.4.1.3 Javacard open platform manufacturing (phase 3) 25
2.4.2 Production 25
2.4.2.1 Javacard open platform (JOP) packaging and initialization (phase 4) 26
2.4.2.2 Javacard open platform (JOP) pre-personnnalization (phase 5) 26
2.4.3 Operational state 27
2.4.3.1 Applet pre-personalisation (phase 6) 27
2.4.3.2 TOE personalisation (phase 6) 27
2.4.3.3 TOE Usage (phase 7) 27
2.4.4 Coverage of the different Life cycle state by the assurance components [AGD] & [ALC] 28
2.4.5 State of the TOE depending on the phase 29
2.4.6 Mapping with the Users 29

3 CONFORMANCE CLAIM 30

3.1 CONFORMANCE CLAIM 30
3.2 PROTECTION PROFILE 30
3.3 CONFORMANCE CLAIM RATIONALE 31
3.3.1 Life cycle conformance 31
3.3.2 Translation from CC v2.1 to CC v3.1 R4 31
3.3.3 SPD statement consistency 31
3.3.3.1 Assets 31
3.3.3.2 Threats 32
3.3.3.3 OSP 33
3.3.3.4 Assumptions 33
3.3.4 Objectives 33

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

3.3.4.1 Security Objectives for the TOE 33
3.3.4.2 Security Objectives for the Operational Environment 34
3.3.5 Users and Remote IT entities 34
3.3.5.1 Users 35
3.3.5.2 Remote IT entities 37
3.3.6 SFR and SAR Statements consistency 39
3.3.6.1 SFR consistency 39
3.3.6.2 SAR consistency 42

4 SECURITY PROBLEM DEFINITION 43

4.1 ASSETS 43
4.2 USERS 44
4.3 REMOTE IT ENTITY 46
4.4 ASSUMPTION 48
4.4.1 Assumption drawn from [SSCD2] and [SSCD3] 48
4.4.2 Complementary Assumption 48
4.5 THREATS 48
4.5.1 Threats drawn from [SSCD2] and [SSCD3] 48
4.5.2 Complementary threats 50
4.6 ORGANIZATIONAL SECURITY POLICIES 51
4.6.1 Organizational security policies drawn from [SSCD2] and [SSCD3] 51
4.6.2 Complementary organizational security policies 51
4.7 SECURITY OBJECTIVES FOR THE TOE 52
4.7.1 Security objectives of the TOE drawn from [SSCD2] and [SSCD3] 52
4.7.2 Complementary security objectives of the TOE 54
4.8 SECURITY OBJECTIVES FOR THE ENVIRONMENT 56
4.8.1 Security objectives of the Environment drawn from [SSCD2] and [SSCD3] 56
4.8.2 Complementary security objectives of the Environment 58

5 EXTENDED REQUIREMENTS 59

5.1 EXTENDED FAMILIES 59
5.1.1 Extended Family FPT_EMSEC - TOE Emanation 59
5.1.1.1 Family behaviour 59
5.1.2 Extended Family FCS_RNG - FCS_RNG: Random Number Generation 60
5.1.2.1 Family behaviour 60

6 SECURITY REQUIREMENTS 62

6.1 SECURITY FUNCTIONAL REQUIREMENTS 62
6.1.1 SFR drawn from the Protection Profile 62
6.1.1.1 Phase 6 and 7 62
6.1.1.2 Phase 7 72
6.1.2 Additional SFRs 77
6.1.2.1 Phase 6 77
6.1.2.2 Phase 7 78
6.1.2.3 Phase 6&7 82
6.2 SECURITY ASSURANCE REQUIREMENTS 91
6.2.1 Evaluation Assurance Level rationale 91
6.2.1.1 ADV : Development 91
6.2.1.2 AGD : Guidance 92
6.2.1.3 ALC : Life cycle 92
6.2.1.4 ASE : Security target 92
6.2.1.5 ATE : Tests 93
6.2.1.6 AVA : Vulnerability 93
6.2.2 Rationale for augmentation 94

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

6.2.2.1 AVA_VAN.5 Advanced methodical vulnerability analysis 94
6.2.2.2 ALC_DVS.2 Sufficiency of security measures 94
6.3 SECURITY REQUIREMENTS RATIONALE 95
6.3.1 Security Objectives of the TOE rationale 95
6.3.1.1 Rationale 95
6.3.2 Security functional requirements analysis 105
6.3.2.1 Dependencies analysis 105
6.3.2.2 Justification for not satisfied dependencies 123
6.3.3 Security Objectives rationale 125
6.3.3.1 Policies and Security Objective Sufficiency 126
6.3.3.2 Threats and Security Objective Sufficiency 127
6.3.3.3 Assumption and Security Objective Sufficiency 131

7 TOE SECURITY SPECIFICATION 132

7.1 DESCRIPTION 132

8 ANNEX A : ATTRIBUTES FOR FDP_ACF SECURITY ATTRIBUTE BASED ACCESS CONTROL 140

8.1 GENERAL ATTRIBUTE 140
8.2 INITIALISATION ATTRIBUTE GROUP 142
8.3 SIGNATURE CREATION ATTRIBUTE GROUP 145
8.4 ADMINISTRATION GROUP 146
8.5 KEY MANAGEMENT GROUP 148

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

1 Introduction

1.1 Security target Reference

The Security target is identified as follows:

Title:	SUCELLOS – Public security target
Reference:	FQR 110 6879 Ed1
Editor:	Oberthur Technologies
CC version:	3.1 revision 4
EAL:	EAL5 augmented with AVA_VAN.5, and ALC_DVS.2

1.2 References

[AN10]	JIL - Certification of "open" smart card products - Version 1.1 - 4 February 2013
[ANSIX9.31]	"Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (DSA)" ANSI X9.31-1998, American Bankers Association
[ANSIX9.62]	ANSI x9.62-2005 Public Key Cryptography for the Financial Services Industry – The Elliptic Curve Digital Signature Algorithm (ECDSA)
[CC31-1]	"Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model", September 2012, Version 3.1 revision 4
[CC31-2]	"Common Criteria for information Technology Security Evaluation, Part 2: Security Functional requirements", September 2012, Version 3.1 revision 4
[CC31-3]	"Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance requirements", September 2012, Version 3.1 revision 4
[FIPS180-3]	"FIPS PUB 180-3, Secure Hash Standard" October 2008 , National Institute of Standards and Technology

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

[GP2.1.1]	Global Platform, Card Specification Version 2.1.1 – March 2003.
[GP2.2.1]	Global Platform, Card Specification Version 2.2.1 – January 2011.
[IASECC]	European Card for e-Services and national e-ID Applications - IAS ECC v1.0.1
[IEEE]	IEEE Std 1363a-2004 Standard Specification of Public-Key Cryptography
[JIL-COMP]	Joint Interpretation Library - Composite product evaluation for Smart Cards and similar devices – v1.2
[Minidriver]	Windows Smart Card Minidriver Specification Version 7.06 July 1, 2009
[PKCS#1]	PKCS #1 v2.1: RSA Cryptography Standard June 14, 2002
[PKCS#3]	PKCS#3 - Diffie-Hellman Key-Agreement Standard Version 1.4, November 1, 1993*
[PLT]	Javacard Open platform certified under reference [ANSSI-CC-2013/09-M01] and [ANSSI-CC-2013/16-M01]
[PP0035]	Security IC Platform Protection Profile Version 1.0 15.06.2007
[TR03111]	Technical Guideline TR-03111 Elliptic Curve Cryptography Version 2.0

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

[RGS_B1]	Référentiel général de sécurité, version 1.0 du 06/05/12 Annexe B1 - Mécanismes cryptographiques
[SCP03]	Global Platform Card Technology, Secure Channel Protocol 03, Card Specification v 2.2 - Amendment D Version 1.1 - September 2009.
[SSCD2]	Secure Signature-Creation Device Type2, 1.04,EAL 4+
[SSCD3]	Secure Signature-Creation Device Type3, 1.05,EAL 4+
[SP800-38B]	NIST Special Publication 800-38B, Recommendation for Block, Cipher Modes of Operation: The CMAC Mode for Authentication, Morris Dworkin, May 2005
[14890]	CEN/EN14890:2013 Application Interface for smart cards used as Secure Signature Creation
[7816-4]	ISO/IEC 7816-4:2013, Identification Cards — Integrated circuit cards— Part 4 : Organization, security and commands for interchange
[9797-1]	ISO/IEC 9797-1:2011, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher
[11568-2]	ISO 11568-2:2012,Financial services - Key management (retail) - Part 2 : symmetric ciphers, their key management and life cycle

1.3 Definitions

ADF Application Dedicated File
AES Advanced Encryption Standard
AID Application Identifier
AMB Access Mode Byte
APDU Application Protocol Data Unit (command received/Data sent by the chip)
API Application Programming Interfaces
CA Certification authority
CBC Cipher Block Chaining

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

CGA	Certificate Generation Authority (Authority in charge of generating the qualified certificate(s))
C/S	Client / Server
CSE	Current Security Environment
DAP	Data Authentication Pattern (enable to ensure integrity & authenticity of javacard package when loaded)
DAPP	Device Authentication with Privacy Protection
DES	Data Encryption Standard
DF	Dedicated File
DH	Diffie Hellman
DTBS	Data to be signed (Sent by the SCA)
DTBS Representation	Representation of the Data to be signed
EAL	Evaluation Assurance Level
EF	Elementary File
EEPROM	Electrically Erasable Programmable Read Only Memory
FID	File identifier
GP	Global Platform
HI	Human Interface (used to enter the RAD and VAD by the user)
IC	Integrated Chip
ICC	Integrated Chip card
IFD	Interface Device
MAC	Message Authentication code
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RAD	Reference Authentication Data (PIN stored)
RCA	Root Certification Authority
ROM	Read Only Memory
RSA	Rivest Shamir Adleman
RSA CRT	Rivest Shamir Adleman – Chinese Remainder Theorem
SCA	Signature creation Application (Application requiring a qualified signature to the chip)
SCB	Security Condition Byte
SCD	Signature Creation Data (Signature key)
SCP	Secure Channel Procotol
SDO	Security Data Object
SE	Security Environment
SHA	Secure hashing Algorithm
SSCD	Secure Signature Creation Device
SSE	Static Security Environment
SSESP	Static Security Environment for Security Policies
SSO	Single Sign On
SVD	Signature Verification Data (Signature Verification key)
TOE	Target of evaluation
URL	Uniform Resource Locator
USB	Universal Serial Bus
VAD	Verification Authentication Data (PIN submitted by the holder)
XML	eXtensible Markup Language

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

2 Target Of Evaluation

2.1 Overview

2.1.1 TOE Type

The Target of Evaluation is a smartcard which is configured as a Secure signature creation Device (SSCD), used to create advanced or qualified signature in the sense of EC/1999/93.

The TOE is a composite product made up of an embedded software developed using javacard technology, composed on a javacard open platform. Both are developed by Oberthur Technologies.

The javacard open platform has already been certified. For more details see [PLT].

The embedded software is made up of four javacard components:

- a javacard Applet ([Applet]);
- a javacard API ([API]);
- two javacard Interfaces ([Interface]);

[Applet] relies on

- [API] which provides a wide range of services enabling to manage the files and cryptographic objects;
- [Interface] which provides the mechanisms for data sharing with other applets;
- Javacard API provided by the underlying javacard open platform;

2.1.2 Logical scope

The TOE is made up of:

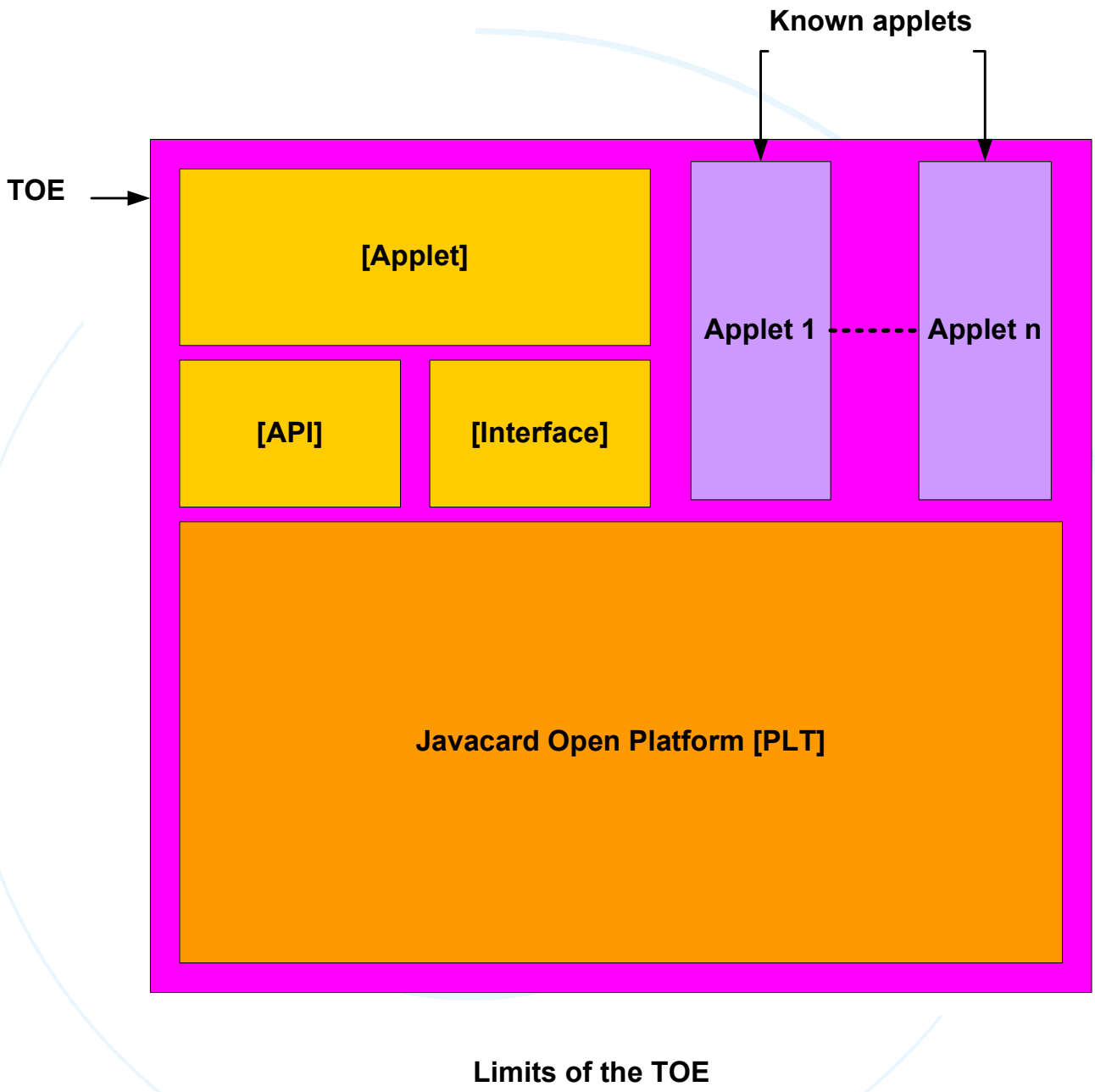
- The underlying javacard open platform
- The javacard code ([Applet], [API] and [Interface])

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

Moreover, as the [PLT] is certified as a javacard open platform and complies with the requirements of the Application note 10 [AN10], and as the TOE complies also with [AN10], the TOE may also contain any other applets that complies with [AN10] and the specific requirements of the TOE stated in the guidance documents.

The logical scope of the TOE may be depicted as follows:

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

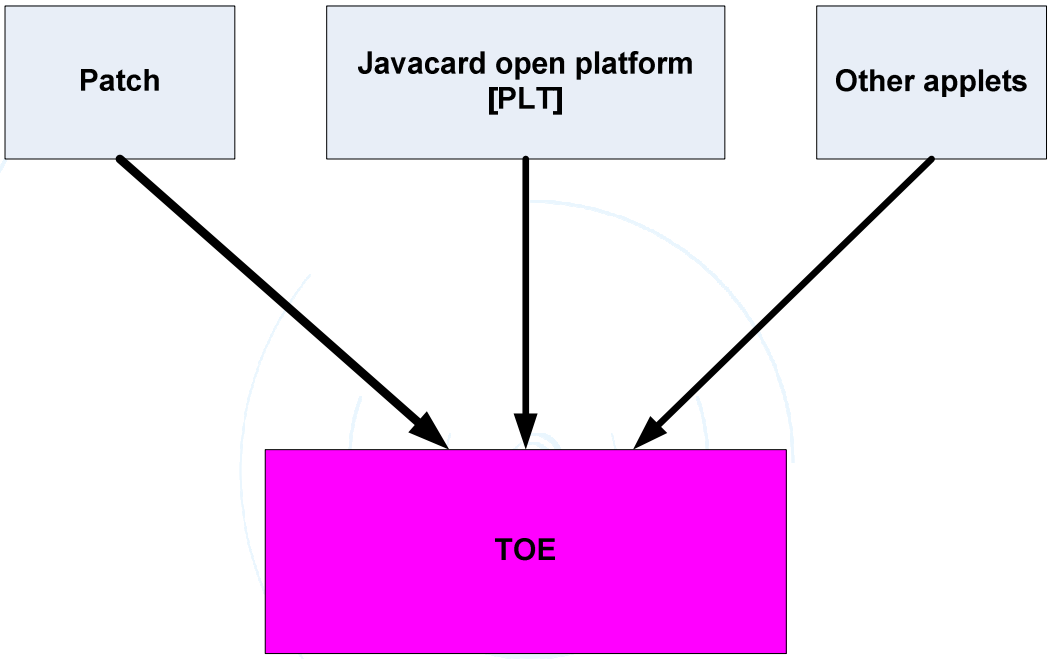


2.1.3 Physical scope

The TOE is physically made up of several components:

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

- the javacard open platform **[PLT],** which contains in its ROM code the javacard packages **[Applet]**, **[API]** and **[Interface]**;
- a potential patch **[patch]** loaded in EEPROM. If a functional patch is required, its reference will be included in a maintenance report;
- the other applets that may potentially be loaded on the javacard open platform **[PLT]** at any time;



Physical scope of the TOE

The patch, if present, is self protected (encrypted and signed). The other applet must fulfil the requirements stated in [AN10] and in the guidance documentation of the TOE.

Once constructed, the TOE is a bare microchip with its external interfaces for communication. The physical medium on which the microchip is mounted is not part of the target of evaluation because it does not alter nor modify any security functions of the TOE.

The TOE may be used on several physical medium

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

- within an inlay, or eCover;
- in a plastic card;
- within a USB key;
- ….;

2.1.4 Required non-TOE hardware/software/firmware

The TOE is a Secure Signature Creation Device. It is an independent product and does not need any additional hardware/software/firmware to ensure its security.

In order to be powered up and to be able to communicate the TOE needs a card reader.

2.1.5 Usage and major security features

The TOE intended usage is to be used as a “secure signature creation device” (SSCD) of type 2 or 3, with respect to the European directive EC/1999/93.

Within the framework described by [SSCD2] and [SSCD3], the TOE allows to

- perform basic, advanced and qualified signature;
- authenticate the cardholder based on a PIN and/or Biometric data verification;
- authenticate one (or several) administrator(s) of the TOE, that may have special rights to administrate the SCD and SVD (generation, import), using either symmetric and/or asymmetric mechanisms, or PIN and/or Biometric data verification;
- establish trusted channel, protected in integrity and confidentiality, with remote entities such as a SCA, a CGA or a SSCD type 1. It may be realized by means of symmetric and/or asymmetric mechanisms;

The scope of [SSCD2] and [SSCD3] is extended in several ways:

- A super Administrator has special rights to administrate the signature creation function, the mode of communication, and the type of cryptographic mechanisms to use.
- The TOE may hold more than one SCD. Several SCDs may be used by the holder to sign documents
- SCD/SVD pairs and other cryptographic objects may be generated and/or imported after issuance at any time, and in particular, they may be updated during the TOE life cycle.
- The TOE may be used to realize digital signature in contact and/or contactless mode.
- eServices features are added, enabling the cardholder to perform C/S authentication, Encryption key decipherment….

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d’Estienne d’Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

- A complete access control over object is ensured, whatever their type is : File or cryptographic objects (PIN, keys,…), ensuring it is not possible to bypass the access rules.

The TOE may be used for various use cases requiring qualified signature:

- Electronic signature application;
- Electronic health card;
- Electronic services cards;
- ……;

Depending on the use case and or the ability of the underlying javacard open platform, the TOE may be used

- in contact mode (T=0 and/or T=1 protocol);
- in contactless protocol (T=CL);

2.1.6 Scope of evaluation

The scope of evaluation covers the following features:

- Features covered by [SSCD2]and [SSCD3]
- Authentication mechanisms based on cryptographic scheme
- Unblocking of RAD
- Management of the other keys (authentication and eservices)

2.2 Description

The TOE is compliant with the specification [IASECC], and is enhanced with the following features:

- The TOE supports user authentication based on Biometric comparison. Two modes of operations, are possible: either a 1:1 Biometric comparison, or a 1:n comparison can be made. These modes of operations are compliant to [14890] and [7816-4]
- The TOE supports Elliptic curves cryptography for electronic signature, encryption key decipherment, and C/S authentication. These modes of operations are compliant to [14890].
- The TOE supports several mode of operation for the data hashing. The data may also be fully hashed on card or off card. These modes of operations are compliant to [14890].
- The TOE supports secure messaging and authentication scheme based on AES block Cipher. These modes of operations are compliant to [14890].
- The TOE supports several features required by [Minidriver]

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

2.2.1 Data structure

The TOE manages two types of structures:

- The File, compliant with [7816-4]
- The Security Data Objects, which are secure container storing cryptographic data (PINs, Keys,….)

2.2.1.1 File and File System

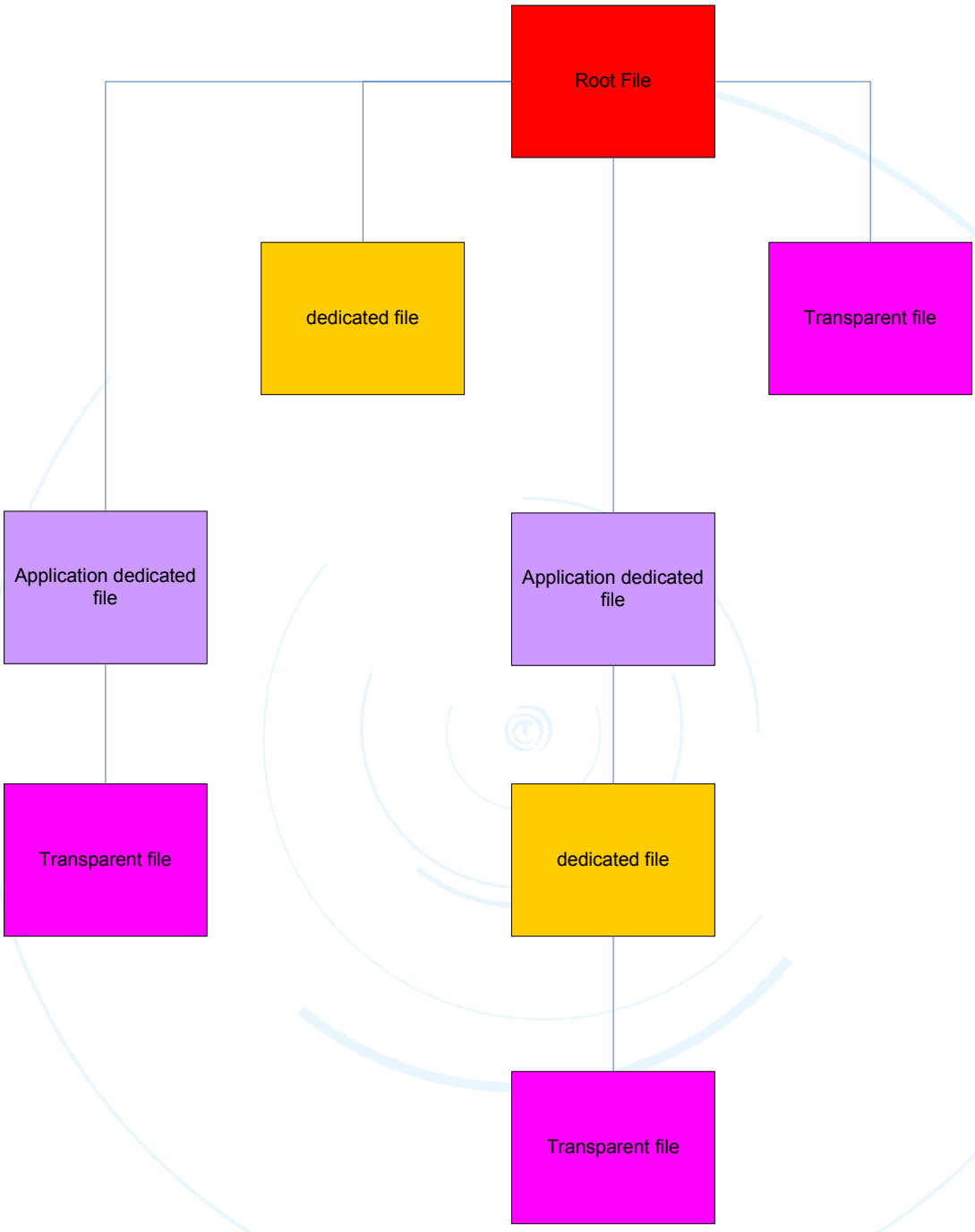
The TOE handles the following type of file (described in [7816-4]):

- Transparent File - EF
- Application Dedicated File - ADF
- Dedicated File - DF

All these files are organized within a File System compliant to [7816-4]. It represents the hierarchy between all the files.

At the top of the structure stands the Root file (or Master File), it is the default selected file at reset. Under the Root file, are located the Application Dedicated File.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534



Example of FileSystem Structure

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

The Root, as well as each ADF and DF, may contain up Elementary File (EF) or Security Data Object (SDO). Each of them may contain up to 255 files (EF or DF) and 31 SDO of each type.

The TOE allows to

- create, delete, activate, deactivate, and terminate any type of file (except the Application dedicated file), which update the File System.
- read, update, resize any transparent file (EF)
- move within the File Structure by use of file selection

Each file is characterised by its own attributes, such as:

- Access conditions
- File identifier
- Location within the File System
- Size (for EF)

The management of the file system is fully described in [IASECC].

2.2.1.2 Security Environment

The TOE handles Security Environments. Three types of Security Environment may be sorted out:

- Static Security Environment - SSE
- Static Security Environment for Security Policies – SSESP
- Current Security Environment - CSE

Basically a security environment contains several couple of cryptographic data, each of them containing:

- One or several key identifier : KEY_ID
- an algorithm identifier : ALGO_ID
- a mode of usage : USE

These cryptographic data may be used to:

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

- load a pre-defined cryptographic context to perform a cryptographic operation (for signature, for C/S authentication,…). It is the case of a SSE.
- define an access condition to fulfil before granting an access right: the key defined by the identifier KEY_ID shall be used with the algorithm ALGO_ID and with the mode USE to grant an access right. It is the case of a SSESP.
- Store the current cryptographic context required to realize a given service. It is the case of the CSE.

The SSESP and SSE are bound to an ADF and are stored in security Data Objects located within an Application dedicated file (ADF). The CSE is unique for the TOE at any moment

2.2.1.3 Security data Objects

The TOE handles as well cryptographic data objects, called Security Data Objects (SDO), dedicated to store the keys, the PIN, the Biometric template, the Diffie Hellmann parameters and the Security Environments, as well as their attributes. The following types of SDO are available:

- SDO PIN contains a Personal identification Number
- SDO BIO contains one or several Biometric template
- SDO RSA Public Key contains a RSA Public Key
- SDO RSA Private Key contains a RSA Private Key
- SDO ECC Public Key contains an ECC Public Key
- SDO ECC Private Key contains an ECC Private Key
- SDO Security Environment contains a Security Environment
- SDO Symmetric DES Key Set contains a Symmetric DES Key Set
- SDO Symmetric AES Key Set contains a Symmetric AES Key Set
- SDO Diffie Hellmann parameters contains a set of Diffie Helmann Domain parameters

The SDO may be located in any dedicated file (DF) or Application Dedicated file (ADF).

The TOE enables to create, update and use any of these SDO. The way the SDO may be used depends on its type:

- SDO PIN and SDO BIO may be changed, reset, verified
- SDO RSA Public Key may be used to verify a certificate
- SDO RSA Private Key and SDO ECC Private key may be used to sign, perform a C/S authentication or decrypt a cryptogram
- SDO Security Environment may be changed, reset, verified

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

- SDO Symmetric DES Key Set and SDO Symmetric AES Key Set may be used to verify an external authentication or to perform a mutual authentication and establish a trusted channel
- SDO Diffie Hellmann parameters may be used to establish a secure channel (without authentication)

Each SDO is characterised by its own attributes, such as:

- Access conditions
- Location within the File System
- Size
- Type
- Secret value
- Usage counter and tries counter
- Algorithm to be used

The management of SDO is fully described in [IASECC].

2.2.2 Access Control Management

One of the Core features of the TOE is to provide access control management on any operations on any objects it handles (Files of SDO).

The Access conditions encoding is the compact encoding described in [7816-4], enhanced as described in [IASECC]. It relies on access rules encoded by means on Access Mode Bytes (AMB) and Security Conditions Bytes (SCB) as described in [7816-4] and [IASECC].

Prior to granting access to a given operation, the TOE checks the requested access rights are fulfilled. Basically, an Access condition is granted if the security conditions are fulfilled. An access condition is a combination of security conditions based on identified keys/PIN/BIO/secrets:

- User Authentication (by PIN or Biometric comparison). It is used to authenticate the cardholder or a remote administrator
- Authentication of a remote administrator
- Mutual authentication with a remote IT
- Communication protected in integrity and confidentiality

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

2.2.3 Authentication of entities

The TOE allows the authentication of several entities in order to grant them some rights.

- User Authentication (by PIN or Biometric comparison). It is used to authenticate the cardholder or a remote administrator
- Authentication of a remote administrator (based on symmetric or asymmetric scheme)
- Mutual authentication with a remote IT and establishment of a trusted channel protected in integrity and confidentiality (based on symmetric or asymmetric scheme)
- Personalisation Agent authentication (for the phase 6)
- TOE Administrator authentication (in phase 7)

These authentication mechanisms are the cornerstone for the access control mechanisms use to grant access to resources (Files or SDO).

2.2.4 Electronic Services

The TOE supports as well several electronic services:

- C/S authentication: this feature enables to authenticate the TOE to a remote entity.
- Digital signature: this feature enables the cardholder to electronically signs documents. The signature may be either advanced or qualified (compliant with [SSCD2] and [SSCD3]).
- Encryption key decipherment: this feature enables the cardholder to store secret data on an electronic vault. The key needed to decipher the key encrypting these data is securely stored in the TOE. The cardholder's computer sends the encrypted encryption key to the TOE to get the plain encryption key.

2.2.5 Administration of the TOE

The TOE offers administration services. Upon successful authentication, the TOE Administrator may modify the following attributes:

- Communication medium: the administrator may restrict the ability to communicate with the TOE in contact and/or contactless mode.
- Hashing method to be used for digital signature: the administrator may restrict the ability to perform electronic signature (advanced or qualified) on DTBS-representation partly computed by the TOE. In such case, the digital signature will only be done with last round of data hashing done on the TOE.
- Authentication mechanism to be used: the administrator may restrict the cryptographic means to be used by the TOE to authenticate remote entities (Administrator or Remote IT): either symmetric and/or asymmetric cryptography.
- Identification of the TOE : the administrator is entitled to identify the TOE
- Biometric threshold : the administrator can modify the biometric threshold

2.2.6 Single Sign on feature (SSO)

The TOE may also behave as a Single Sign on (SSO). It provides access points to any other applet willing to use authentication services based on a PIN stored in the Root File (or Master File). In particular it is possible to:

- Check a PIN
- Change a PIN
- Reset a PIN
- Retrieve the remaining tries counter

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

- Retrieve the validation status

This feature is used for instance when the PIN(s) is shared with a legacy application. Even though the TOE offers these entry points, it does still enforce access control in the same way it does when it receives incoming APDU to use a PIN.

2.3 Reference

The TOE is identified as follows:

TOE name (commercial name):	IAS ECC v2 R1 on ID-One Cosmo V7.1-s Card (Standard Dual and Basic Dual)
Guidance document for preparation	FQR 110 6816 Ed3 – SUCELLOS – AGD_PRE
Guidance document for operational use	FQR 110 6863 Ed2 - SUCELLOS - AGD_OPE
Guidance document for preparation of Platform	FQR 110 6027 - ID-One Cosmo V7.1 - Pre-Perso Guide
Guidance document for operational use of Platform	FQR 110 6028 - ID-One Cosmo V7.1 - Reference Guide FQR 110 6268 - ID-One Cosmo V7.1 - Applications on ID-ONE COSMO V7.1 FQR 110 6319 - ID-One Cosmo V7.1 - All Applications on ID-ONE COSMO V7.1 FQR 110 6267 - ID-One Cosmo V7.1 - Application Loading Protection Guidance FQR 110 6029 - ID-One Cosmo V7.1 - Security Recommendations

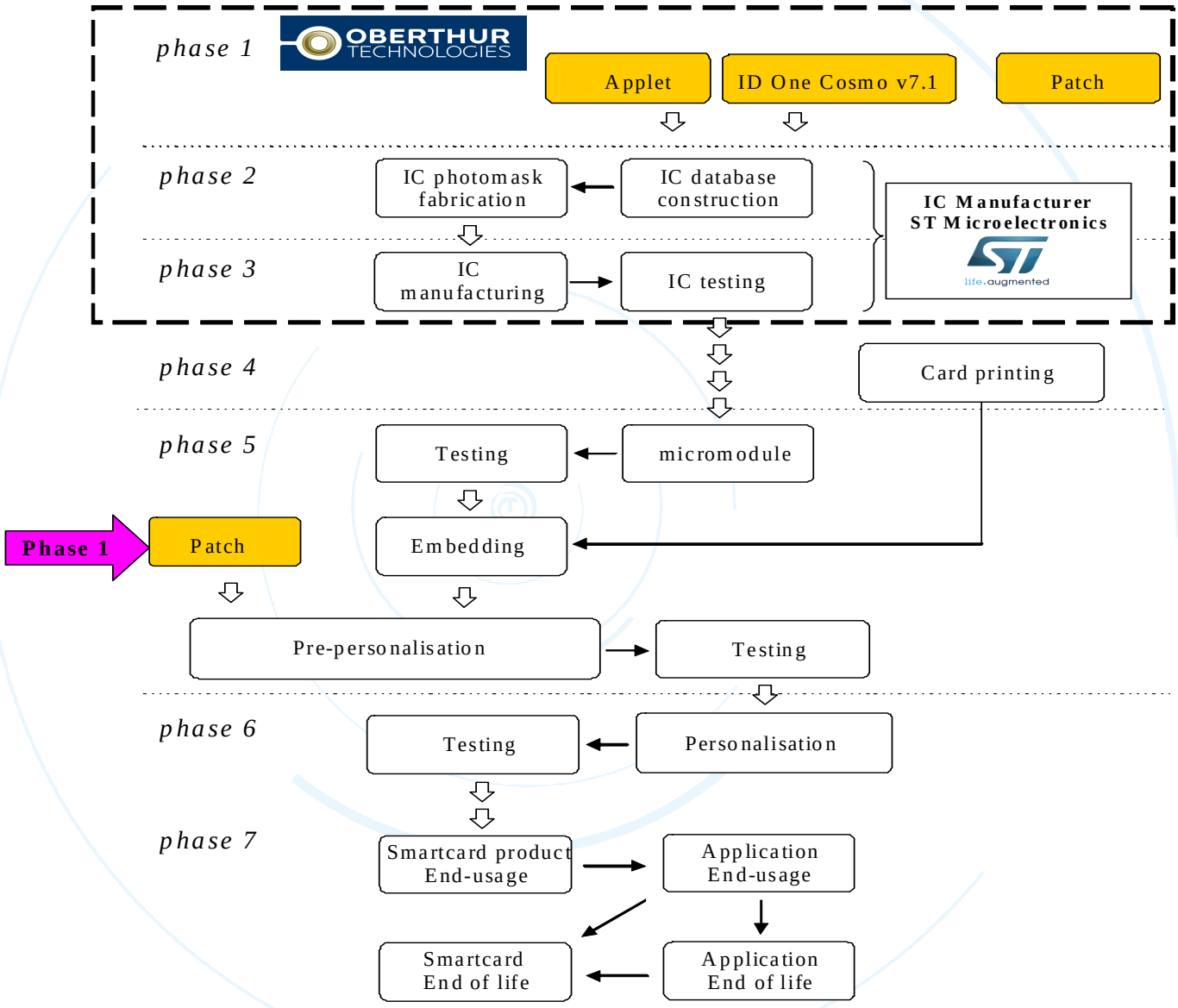
Software identification	'D0010209'

Name of [PTL]	Plateforme JavaCard de la carte à puce ID-One Cosmo V7.1-s sur composants ST23YR80B (Standard Dual) et ST23YR48B (Basic Dual)
Certificate	ANSSI-CC-2013/16-M01

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

2.4 Life Cycle

With respect to the Life cycle envisioned in [PP0035], seven different phases may be sorted out. The life cycle of the composite TOE may be depicted as follows:



The point of delivery of the TOE is the end of phase 3. At this moment, the TOE is self protected, but not constructed.
The point of delivery of the personalisation key required to authenticate with the TOE in phase 6, is the end of phase 5.

The TOE Life cycle may be splitted in three steps

- Development (phase 1 to 3);

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

- Production (phase 4 and 5);
- Operational state (phase 6 and 7);

2.4.1 Development

The development of the TOE takes place in phase 1 to 3. In this step, the parts of TOE are designed, tested and manufactured. This step is covered by [ALC] tasks.

2.4.1.1 Software development (phase 1)

This development environment of the Javacard Applet, the patch if any and javacard open platform (JOP) is enforced by OBERTHUR TECHNOLOGIES.

The confidentiality and integrity of the cap files, the patch and of the javacard open platform is covered by the evaluation of the development premises of OBERTHUR TECHNOLOGIES.

To ensure security, access to development tools and products elements (PC, card reader, documentation, source code...) is protected. The protection is based on measures for prevention and detection of unauthorized access. Two levels of protection are applied:

- Access control to OBERTHUR TECHNOLOGIES offices and sensitive areas.
- Access to development data through the use of a secure computer system to design, implement and test software

At the end of this phase, the code of the javacard applet is delivered to the javacard open platform development team, in order to be stored in the ROM code. The software development phase of the javacard open platform is covered by [PLT].

2.4.1.2 Hardware development (Phase 2)

In this phase, the underlying integrated circuit is developped. This phase takes place at the manufacturing site of the silicium provider.

The confidentiality and integrity of the javacard packages and javacard open platform is covered by the evaluation of the development premises of the silicium manufacturer (see [PLT])

2.4.1.3 Javacard open platform manufacturing (phase 3)

In this phase, the code of the javacard open platform (JOP) and the applet are masked on the IC. This phase takes place at the manufacturing site of the silicium provider.

The confidentiality and integrity of the javacard packages and javacard open platform is covered by the evaluation of the development premises of the silicium manufacturer (see [PLT]).

Depending on the choice made for the optional code loading, it may be loaded during this phase.

At the end of phase 3, the javacard open platform (JOP) and the TOE are self protected: all its security functions are activated. The point of delivery of the TOE is the end of phase 3.

2.4.2 Production

The production environment encompasses the preparation of the TOE and the management of the personalisation key used to personalize it.

During this step, the following operations are made:

- The chip is mounted on a physical layout (card, USB token...)
- The javacard open platform is prepersonalized
- The javacard open platform is personalized
- The personalisation key is loaded on the TOE
- The applet is instantiated
- The applet is pre-personnalized

This step is covered by [AGD_PRE] tasks for the TOE, and by [ALC] for the management of the personalisation key in its environment.

2.4.2.1 Javacard open platform (JOP) packaging and initialization (phase 4)

This phase is performed by the Manufacturing Agent, which controls the TOE, that is in charge of the packaging and initialization of the Javacard open platform (JOP).

This phase spans the phase 4 of the Javacard open platform (JOP) life cycle and is covered by [AGD_PRE] tasks of [PLT].
All along this phase, the TOE is self-protected as it requires the authentication of the Manufacturing Agent prior to any operation.

2.4.2.2 Javacard open platform (JOP) pre-personnnalization (phase 5)

This phase is performed by the Manufacturing Agent, which controls the TOE, in the manufacturing site of Vitré (France – 35). The procedures and the IT infrastructure ensure the integrity and authenticity of the keys used to get authenticated with the TOE.

This phase spans the following phases of the javacard open platform (JOP):

- Phase 5
- Phase 6
- Phase 7

The following process is applied during this phase

- a non-security patch [patch] (patch code that has no impacts on product auto-protection) is loaded in the javacard open platform (JOP) in phase 5 (if needed);
- the javacard open platform (JOP) is switched in phase 5 and the applet may be instantiated in this phase;
- the javacard open platform (JOP) is switched in phase 6 and the applet may be instantiated in this phase;
- the javacard open platform (JOP) is switched in phase 7 and the applet may be instantiated in this phase;

Before the patch is loaded in the javacard open platform, the TOE is made of two elements (the patch and the javacard open platform). Once it is loaded, the TOE is the single javacard open platform containing the patch. Moreover, during this phase, any other applet may be loaded at any time (phase 5, 6 or 7 of the javacard open platform), provided they fulfil the requirements laid down in [AN10]. At the end of this phase, the javacard open platform is switched in phase 7 (DAP enforced)

All along this phase, the TOE is self-protected as it requires the authentication of the Manufacturing Agent prior to any operation.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

2.4.3 Operational state

2.4.3.1 Applet pre-personalisation (phase 6)

This phase is performed by the Personalisation Agent, which controls the TOE. During this phase, the javacard applet is prepared as required by P.TOE_Construction.

All along this phase, the TOE is self-protected as it requires the authentication of the Personalisation Agent prior to any operation.

2.4.3.2 TOE personalisation (phase 6)

This phase is performed by the Personalisation Agent, which controls the TOE, which is in charge of the javacard applet personalisation.

All along this phase, the TOE is self-protected as it requires the authentication of the Personalisation Agent prior to any operation.

This phase may not necessarily take place in a manufacturing site, but may be performed anywhere. The Personalisation Agent is responsible for ensuring a sufficient level of security during this phase.

The javacard applet is personalized according to [AGD_PRE], and the following operations are made: creation of applicative data (SCD, SVD, RAD, File,…) and the TOE_Administrator Agent key is loaded.

At the end of phase 6, the TOE is constructed

2.4.3.3 TOE Usage (phase 7)

The TOE is under the control of the User (Signatory and/or Administrator) and TOE_Administrator.

During this phase, the TOE may be used to create a secure signature and manage the SCD, the SVD and the RAD.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

2.4.4 Coverage of the different Life cycle state by the assurance components [AGD] & [ALC]

The following phases of the life cycle are covered as follows:

Steps	Life cycle State	TOE : covered by	Personalisation key : covered by
Development	Phase 1	ALC [PLT] ALC [SUCELLOS]	N/A
	Patch is self protected		
	Phase 2	ALC [PLT] ALC [SUCELLOS]	N/A
	Phase 3	ALC [PLT] ALC [SUCELLOS]	N/A
Patch is loaded TOE is self protected			
Point of delivery of the TOE			
Production	Phase 4	AGD_PRE [PLT]	N/A
	Phase 5	AGD_PRE [PLT] AGD_OPE [PLT]	ALC [SUCELLOS]
Point of delivery of the personalisation key			
Patch is loaded			
Operational	Phase 6	AGD_OPE [PLT] AGD_PRE [SUCELLOS]	N/A
	TOE is constructed		
	Phase 6	AGD_OPE [PLT] AGD_PRE [SUCELLOS]	N/A
	Phase 7	AGD_OPE [PLT] AGD_PRE [SUCELLOS]	N/A

The point of delivery of the TOE is the end of phase 3, and the point of delivery of the personalisation key is the end of phase 5. The security of the patch loading (done after phase 3) is fully enforced by technical security measures that have been evaluated in [PLT]. Therefore, phase 4 to 6 are fully covered by [AGD_PRE] and [AGD_OPE], except the personalisation key management in the environment which is covered by [ALC].

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

2.4.5 State of the TOE depending on the phase

Life cycle State	TOE		Personalisation key	
	Self protected	constructed	stored in	Protected by
Phase 1	**No**	**No**	**N/A**	**N/A**
Phase 2	**No**	**No**	**N/A**	**N/A**
Phase 3	**No**	**No**	**N/A**	**N/A**
Phase 4	**Yes**	**No**	**N/A**	**N/A**
Phase 5	**Yes**	**No**	**Manufacturing centre**	**ALC[SUCELLOS]**
Phase 6	**Yes**	**Yes**	**N/A**	**N/A**
Phase 7	**Yes**	**Yes**	**N/A**	**N/A**

2.4.6 Mapping with the Users

For each of these phases, the following subjects may interact with the TOE

Life cycle phase	Subject interacting with the TOE
Phase 1	OBERTHUR TECHNOLOGIES
Patch ,if it exists, is self protected	
Phase 2	OBERTHUR TECHNOLOGIES
Phase 3	OBERTHUR TECHNOLOGIES
TOE is self protected	
Phase 4	Manufacturing Agent Offcard
Phase 5	Manufacturing Agent Offcard
Phase 6	Personalisation Agent Offcard
TOE is constructed	
Phase 6	Personalisation Agent Offcard
Phase 7	Users

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

3 Conformance Claim

3.1 Conformance claim

This security target claims conformance to the Common Criteria version 3.1, revision 4 ([CC31-1], [CC31-2] and [CC31-3]).

The conformance to the Common Criteria is claimed as follows:

CC	Conformance rationale
Part 1	Strict Conformance
Part 2	Conformance to the extended part. ▪ FCS.RNG.1: "Random number generation" ▪ FPT_EMSEC.1: "TOE Emanation"
Part 3	Conformance to EAL 5, augmented with ▪ AVA_VAN.5: *"Advanced methodical vulnerability analysis"* ▪ ALC_DVS.2: *"Sufficiency of security measures"*

Moreover the security target claims compliance with Application note 10 [AN10].

3.2 Protection Profile

This security target claims a **demonstrable** conformance to the Secure Signature Creation Device (SSCD) Protection Profile [SSCD2] and [SSCD3].

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

3.3 Conformance Claim rationale

3.3.1 Life cycle conformance

The life cycle of the TOE is described in §2.4. This chapter demonstrates the mapping of the TOE's life cycle with the one described in [SSCD2] and [SSCD3].

Life cycle phase of the TOE	Life cycle phase with respect to [SSCD2] and [SSCD3]
Phase 1	Design
Patch is self protected	
Phase 2	Fabrication
Phase 3	Fabrication
TOE is self protected	
Phase 4	N/A
Phase 5	Loading of application data
Patch is loaded on the Javacard open platform TOE is self protected	
Phase 6	Loading of application data
TOE is constructed	
Phase 6	Personalisation
Phase 7	Usage Destruction

3.3.2 Translation from CC v2.1 to CC v3.1 R4

[SSCD2] and [SSCD3] were written in CC v2.1 methodology. The current security target is based on these Protection profiles and was upgraded to take into account the latest version of the common criteria (CC v3.1).

The conformity of the security target to these protection profiles is demonstrated hereafter.

3.3.3 SPD statement consistency

3.3.3.1 Assets

All assets from the protection profiles [SSCD2] and [SSCD3] are included in the security target. However, their classifications have been upgraded as follows:

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

Data	Property	Type of data
SCD:	Integrity, confidentiality	User Data
SVD	Integrity	User Data
DTBS and DTBS-representation	Integrity	User Data
VAD	Integrity, confidentiality as needed by authentication method	TSF data Its integrity and confidentiality is ensured by OE.HI_VAD
RAD	Integrity, confidentiality	TSF Data Its integrity and confidentiality is ensured by the TOE
Signature-creation function of the SSCD using the SCD	-	TSF
Electronic signature	-	As it is an electronic signature, it is protected in integrity

3.3.3.2 Threats

All threats from the protection profiles [SSCD2] and [SSCD3] are included in the security target. The following threats have been added:

Threat	Rationale
T.Key_Divulg	Storing ,copying, and releasing of a key stored in the TOE
T.Key_Derive	Derive a key
T.TOE_PublicAuthKey_Forgery	Forgery of the public key of a TOE authentication key

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

Threat	Rationale
T.Authentication_Replay	Replay of an authentication of an external entity

3.3.3.3 OSP

All OSPs from the protection profiles [SSCD2] and [SSCD3] are included in the security target. The following OSP have been added:

OSP	Rationale
P.LinkSCD_QualifiedCertificate	Link between a SCD stored in the TOE and the relevant qualified certificate
P.TOE_PublicAuthKey_Cert	Certificate for asymmetric TOE authentication keys
P.TOE_Construction	Construction of the TOE by the Personnalization Agent
P.eServices	Provision of eServices

3.3.3.4 Assumptions

The assumption from the protection profile are included in the security target, no additional assumptions have been added.

3.3.4 Objectives

3.3.4.1 Security Objectives for the TOE

All security objectives for the TOE from the protection profiles [SSCD2] and [SSCD3] are included in the security target. The following security objectives for the TOE have been added:

Security Objectives for the TOE	Rationale
OT.Authentication_Secure	Secure authentication mechanisms
OT.SCD/SVD_Management	Management of SCD/SVD

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

Security Objectives for the TOE	Rationale
OT.Key_Lifecycle_Security	Lifecycle security of the key(s) stored in the TOE
OT.Key_Secrecy	Secrecy of the key(s) stored in the TOE
OT.TOE_AuthKey_Unique	Uniqueness of the TOE authentication key(s)
OT.LifeCycle_Management	Management of the life cycle
OT.eServices	Provision of eServices

3.3.4.2 Security Objectives for the Operational Environment

All security objectives for the Operational Environment from the protection profiles [SSCD2] and [SSCD3] are included in the security target. The following security objectives for the Operational Environment have been added:

Security Objectives for the TOE	Rationale
OE.LinkSCD_QualifiedCertificate	Link between a SCD stored in the TOE and the relevant qualified certificate
OE.AuthKey_Transfer	Secure transfer of Authentication key(s) to the TOE
OE.AuthKey_Unique	Uniqueness of the authentication key(s)
OE.TOE_PublicAuthKey_Transfer	Secure transfer of Public Authentication key(s) of the TOE
OE.TOE_Construction	Construction of the TOE by the Personalisation Agent

None of these new environment objectives interfere with the security problem definition stated by [SSCD2] and [SSCD3].

3.3.5 Users and Remote IT entities

The current security target considers supplemental Users and Remote IT entities.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

3.3.5.1 Users

The current security target envisions the following users:

- Signatory
- Personalisation Agent
- User_Admin
- SCA
- CGA
- SSCD type 1
- TOE_Administrator

However, these users may be sorted out according to the classification described in [SSCD2] and [SSCD3] as follows:

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

Users	Remark	Phases in which it is active	Mapping with [SSCD2] and [SSCD3]	Drawn from [SSCD2] and [SSCD3]?
Signatory	Natural user to which the signature functionality is reserved	7	User Signatory	Y
Personalisation Agent	User in charge of the personalisation in phase 6	6	User Administrator	Y
User_Admin	User with administrative right in phase 7	7	User Administrator	Y
SCA	Signature creation application	7	Depending on the use case, and the TOE preparation (see [AGD_PRE]) , this user may be a User, Administrator	Y
CGA	Certificate Generation Application	7	Depending on the use case, and the TOE preparation (see [AGD_PRE]) , this user may be a User, Administrator	Y
SSCD Type 1	Secure Signature Creation Device of Type 1	7	Depending on the use case, and the TOE preparation (see [AGD_PRE]) , this user may be a User, Administrator	Y
SCA	Signature	7	Supplemental_User	N

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

	creation application			
CGA	Certificate Generation Application	7	Supplemental_User	N
SSCD Type 1	Secure Signature Creation Device of Type 1	7	Supplemental_User	N
IFD	Interface Device. This user is a generic user that may be the SCA, the CGA or the SSCD type 1	7	Supplemental_User	N
TOE_Administrator	Administrator of the TOE in phase 7	7	Supplemental_User	N

The security target considers also the Reomte IT entities “SCA”, “CGA” and “SSCD type 1” as Users of the TOE. The users “SCA”, “CGA”, “SSCD type 1” may be included in the user “Administrator” in the sense of [SSCD2] and [SSCD3] depending on the configuration of the TOE.

3.3.5.2 Remote IT entities

The current security target envisions the following remote IT entities:

- SCA
- CGA
- SSCD type 1
- IFD

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d’Estienne d’Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

Users	Remark	Phases in which it is active	Drawn from [SSCD2] and [SSCD3]?
SCA	Signature creation application. In phase 6, this remote IT entity is mingled with the Personalisation Agent.	6&7	Y
CGA	Certificate Generation Application. In phase 6, this remote IT entity is mingled with the Personalisation Agent.	6&7	Y
SSCD Type 1	Secure Signature Creation Device of Type 1. In phase 6, this remote IT entity is mingled with the Personalisation Agent.	6&7	Y
IFD	Interface Device. This remote IT entity is a generic one that may be the SCA, the CGA or the SSCD type 1	7	N

The remote IT entity “IFD” is a generic one that may be any of the three ones defined by [SSCD2] and [SSCD3].

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d’Estienne d’Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

3.3.6 SFR and SAR Statements consistency

3.3.6.1 SFR consistency

Translation from CC v2.1 to CC v3.1

All the SFRs from the Protection Profile are present in the security target. However, as they are based on previous Common Criteria version (v2.1), some requirements are adapted to CC v3.1 (mainly wording) as well as some dependencies that were modified. In particular, the following upgrade had to be done when migrating from CCv2.1 to CC v3.1:

- FMT_SMF.1 is added as it is now a dependency of FMT_MSA.1, FMT_MOF.1, and FMT_MTD.1
- FPT_AMT is replaced by FPT_TEE.

Withdraw of useless SFRs

FPT_TEE is non applicable in the case of our TOE. With respect to the definition of this SFR, it implies the TOE to perform test on external entities. However, as the TOE does not rely on any external mechanisms to realize the security services and as all the security features are present in the TOE scope, this SFR is non applicable and is withdrawn from the current security target.

Addition of new SFRs

Moreover, SFRs were added to cover supplemental features. The table below lists all the supplemental SFRs that have been added in the security target.

SFRs	Rationale
FCS CKM.1 / Session keys	Generation of secure messaging session keys
FCS_CKM.4 / Session keys	Destruction of secure messaging session keys
FCS_COP.1/ Diffie Hellman computation	Cryptographic operation : Diffie Hellman

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

SFRs	Rationale
FCS_COP.1/ Secure Messaging in Confidentiality	Cryptographic operation : protection in confidentiality of APDU
FCS_COP.1/ Secure Messaging in Integrity	Cryptographic operation : protection in integrity and authenticity of APDU
FCS_COP.1/ Data hashing	Cryptographic operation : Data hashing
FCS_COP.1/ C/S Authentication	Cryptographic operation : C/S Authentication
FCS_COP.1/ Encryption key decipherment	Cryptographic operation : Encryption key decipherment
FCS_COP.1/ Symmetric Role Authentication	Cryptographic operation : symmetric role authentication
FCS_COP.1/ Symmetric Device Authentication	Cryptographic operation : symmetric device authentication
FCS_COP.1/ Certificate Verification	Cryptographic operation : Certificate verification
FCS_COP.1/ Asymmetric Role Authentication	Cryptographic operation : asymmetric role authentication
FCS_COP.1/ Asymmetric Internal DAPP Authentication	Cryptographic operation : asymmetric internal DAPP Authentication
FCS_COP.1/ Asymmetric External DAPP Authentication	Cryptographic operation : asymmetric external DAPP Authentication

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

SFRs	Rationale
FCS_COP.1/ GP Authentication	Cryptographic operation : GP authentication
FCS_COP.1/ GP secret data protection	Cryptographic operation : GP secret data protection
FCS_RNG.1 / Random Number Generation	Cryptographic operation : Random number generation
FDP_ACC.1/IAS ECC Administration SFP	Access control policy for the administration operation of IAS ECC
FDP_ACC.1/Key Management SFP	Access control policy for the key management operations
FDP_ACF.1/ IAS ECC Administration SFP	Access control rules for the administration operation of IAS ECC
FDP_ACF.1/ Key Management SFP	Access control rules for the key management operations
FDP_ETC.1/ Keys transfer	Export of keys
FDP_ITC.1/ Keys	Import of keys
FIA AFL.1/ Authentication keys	Management of wrong authentication with mechanisms based on cryptographic keys
FIA ATD.1 / S.Admin, S.TOE_Admin, S.Personalizer	Association of users with cryptographic keys.
FMT_MSA.1/ Management of TOE	Management of Access rights for IAS ECC administration operations
FMT_MSA.1/ Key Management	Management of Access rights for key management operations
FMT_MTD.1/ Admin	Creation of secure container by the administrator

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

SFRs	Rationale
FMT_MTD.1/ Association between SCD and SCD_ID	Link between a SCD and an identifier
FMT_MTD.1/ TOE Serial number	Loading of the TOE serial number
FMT_MTD.1 / TOE State	Transition of the life cycle of the TOE from phase 6 to phase 7
FMT_MTD.1 / Unblock	Unlocking of RAD by the administrator
FMT_SMF.1	Specification of management functions

3.3.6.2 SAR consistency

[SSCD2] and [SSCD3] require an assurance level of level EAL4 augmented with AVA_MSU.3 and AVA_VLA.4. This assurance level is equivalent to the EAL4 package augmented with AVA_VAN.5.

This security target considers an assurance level EAL5 augmented with AVA_VAN.5 and ALC_DVS.2, which still complies with the requirements of the protection profiles.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

4 Security Problem Definition

4.1 Assets

The assets to be protected by the TOE and its environment within phase 6 and 7 of the TOE's life-cycle are the user data and TSF data defined as follows:

User Data	Property	Definition
SCD:	Integrity, confidentiality	Private key used to perform an electronic signature operation (confidentiality of the SCD must be maintained).
SVD	Integrity	Public key linked to the SCD and used to perform an electronic signature verification (integrity of the SVD when it is exported must be maintained).
DTBS and DTBS-representation	Integrity	Set of data, or its representation which is intended to be signed (Their integrity must be maintained).

TSF Data	Property	Definition
RAD	Integrity, confidentiality	Reference PIN code or biometrics authentication reference used to identify and authenticate the End User (integrity and confidentiality of RAD must be maintained)
VAD	-	PIN code or biometrics data entered by the End User to perform a signature operation (confidentiality and authenticity of the VAD as needed by the authentication method employed)
Keys (secret or private)	Integrity, confidentiality	Private or Secret keys used to authenticate an external user or entity, or to performed eServices
Public key	Integrity	Public key used to perform eServices

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

4.2 Users

The table below identifies the different users that can interact with the TOE. For each of them, this table indicates:

- The phase in which the user is active
- The matching user in the sense of [SSCD2] and [SSCD3]

Users	Remark	Phases in which it is active	Mapping with [SSCD2] and [SSCD3]	Drawn from [SSCD2] and [SSCD3]?
Signatory	Natural user to which the signature functionality is reserved	7	User Signatory	Y
Personalisation Agent	User in charge of the personalisation in phase 6	6	User Administrator	Y
User_Admin	User with administrative right in phase 7	7	User Administrator	Y
SCA	Signature creation application	7	Depending on the use case, and the TOE preparation (see [AGD_PRE]) , this user may be a User, Administrator	Y
CGA	Certificate Generation Application	7	Depending on the use case, and the TOE preparation (see [AGD_PRE]) , this user may be a User, Administrator	Y

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

SSCD Type 1	Secure Signature Creation Device of Type 1	7	Depending on the use case, and the TOE preparation (see [AGD_PRE]) , this user may be a User, Administrator	Y
SCA	Signature creation application	7	Supplemental_User	N
CGA	Certificate Generation Application	7	Supplemental_User	N
SSCD Type 1	Secure Signature Creation Device of Type 1	7	Supplemental_User	N
IFD	Interface Device. This user is a generic user that may be the SCA, the CGA or the SSCD type 1	7	Supplemental_User	N
TOE_Administrator	Administrator of the TOE in phase 7	7	Supplemental_User	N

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

4.3 Remote IT entity

The table below identifies the different remote IT entities that can interact with the TOE. For each of them, this table indicates the phase in which it is active.

Users	Remark	Phases in which it is active	Drawn from [SSCD2] and [SSCD3]?
SCA	Signature creation application. In phase 6, this remote IT entity is mingled with the Personalisation Agent.	6&7	Y
CGA	Certificate Generation Application. In phase 6, this remote IT entity is mingled with the Personalisation Agent.	6&7	Y
SSCD Type 1	Secure Signature Creation Device of Type 1. In phase 6, this remote IT entity is mingled with the Personalisation Agent.	6&7	Y
IFD	Interface Device. This remote IT entity is a generic one that may be the SCA, the CGA or the SSCD type 1	7	N

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

WWW.OBERTHUR.COM

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com

S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

4.4 Assumption

4.4.1 Assumption drawn from [SSCD2] and [SSCD3]

A.CGA	Trustworthy certification-generation application

The CGA protects the authenticity of the signatory's name and the SVD in the qualified certificate by an advanced signature of the CSP.

A.SCA	Trustworthy signature-creation application

The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS-representation of data the signatory wishes to sign in a form appropriate for signing by the TOE.

A.SCD_Generate	Trustworthy SCD/SVD generation

If a party other than the signatory generates the SCD/SVD-pair of a signatory, then

(a) this party will use a SSCD for SCD/SVD-generation,

(b) confidentiality of the SCD will be guaranteed until the SCD is under the sole control of the signatory and

(c) the SCD will not be used for signature-creation until the SCD is under the sole control of the signatory.

(d) The generation of the SCD/SVD is invoked by authorised users only

(e) The SSCD Type1 ensures the authenticity of the SVD it has created and exported

4.4.2 Complementary Assumption

N/A

4.5 Threats

4.5.1 Threats drawn from [SSCD2] and [SSCD3]

T.Hack_Phys	Physical attacks through the TOE interfaces

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

An attacker interacts with the TOE interfaces to exploit vulnerabilities, resulting in arbitrary security compromises. This threat addresses all the assets.

T.SCD_Divulg	**Storing ,copying, and releasing of the signature-creation data**

An attacker can store, copy the SCD outside the TOE. An attacker can release the SCD during generation, storage and use for signature-creation in the TOE.

T.SCD_Derive	**Derive the signature-creation data**

An attacker derives the SCD from public known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data communicated outside the TOE, which is a threat against the secrecy of the SCD.

T.Sig_Forgery	**Forgery of the electronic signature**

An attacker forges the signed data object maybe together with its electronic signature created by the TOE and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature generated by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

T.Sig_Repud	**Repudiation of signatures**

If an attacker can successfully threaten any of the assets, then the non repudiation of the electronic signature is compromised. The signatory is able to deny having signed data using the SCD in the TOE under his control even if the signature is successfully verified with the SVD contained in his un-revoked certificate.

T.SVD_Forgery	**Forgery of the signature-verification data**

An attacker forges the SVD presented by the TOE. This result in loss of SVD integrity in the certificate of the signatory.

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

T.DTBS_Forgery	**Forgery of the DTBS-representation**

An attacker modifies the DTBS-representation sent by the SCA. Thus the DTBS-representation used by the TOE for signing does not match the DTBS the signatory intends to sign.

T.SigF_Misuse	**Misuse of the signature-creation function of the TOE**

An attacker misuses the signature-creation function of the TOE to create Signed Data Object for data the signatory has not decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

4.5.2 Complementary threats

T.Key_Divulg	**Storing ,copying, and releasing of a key stored in the TOE**

An attacker can store, copy an authentication or eService key stored in the TOE outside the TOE. An authentication key may be either used to authenticate an external entity or the TOE, and may be symmetric or asymmetric. An attacker can release an authentication or eService key during generation, storage and use in the TOE.

T.Key_Derive	**Derive a key**

An attacker derives an authentication key (of the TOE or an external entity) or eService key from public known data, such as the corresponding public key or cryptogram created by means of the key or any other data communicated outside the TOE, which is a threat against the secrecy of the key.

T.TOE_PublicAuthKey_Forgery	**Forgery of the public key of a TOE authentication key**

An attacker forges the public key of a TOE authentication key presented by the TOE. This results in loss of the public key integrity in the authentication certificate of the TOE.

T.Authentication_Replay	**Replay of an authentication of an external entity**

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

An attacker retrieves by observation authentication data used by a third party during an authentication sequence. The attacker tries to replay this authentication sequence to grant access to the TOE.

4.6 Organizational security policies

4.6.1 Organizational security policies drawn from [SSCD2] and [SSCD3]

P.CSP_QCert	**Qualified certificate**

The CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD. The qualified certificates contains at least the elements defined in Annex I of the Directive, i.e., inter alia the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE is evident with signatures through the certificate or other publicly available information.

P.QSign	**Qualified electronic signatures**

The signatory uses a signature-creation system to sign data with qualified electronic signatures. The DTBS are presented to the signatory by the SCA. The qualified electronic signature is based on a qualified certificate and is created by a SSCD.

P.Sigy_SSCD	**TOE as secure signature-creation device**

The TOE stores the SCD used for signature creation under sole control of the signatory. The SCD used for signature generation can practically occur only once.

4.6.2 Complementary organizational security policies

P.LinkSCD_QualifiedCertificate	**Link between a SCD stored in the TOE and the relevant qualified certificate**

The Subject in charge of creating and updating the SCD (**Personalisation Agent**, **Administrator**, **Signatory**), or the remote IT entity involved in the updating process (the **SSCD,** the **CGA)** shall ensure an unambiguous link between the (qualified) certificate(s) and the matching SCD(s). This link might be figured out by a PKCS#15 structures, an XML structure, an identifier .linking the file containing the (qualified) certificate or the URL hosting them to the SCD(s) loaded in the TOE. In particular, it implies this link updated, each time the SCD(s) is created, imported, erased or generated.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

P.TOE_PublicAuthKey_Cert	Certificate for asymmetric TOE authentication keys

The TOE contains certificate(s) issued by a known entity ensuring its public key corresponding to its private key used for authentication is genuine.

P.TOE_Construction	Construction of the TOE by the Personalisation Agent

The recommendations indicated in [**AGD_PRE**] required to construct the TOE are correctly applied.

P.eServices	Provision of eServices

The TOE provides eServices Mechanisms enabling to:

- decrypt encryption keys
- authenticate the TOE
- verify CVC certificates

Moreover the TOE ensures the key its uses are genuine by enforcing an access control over the keys update, in order to ensure that only entitled entities can change key values.

4.7 Security Objectives for the TOE

4.7.1 Security objectives of the TOE drawn from [SSCD2] and [SSCD3]

OT.EMSEC_Design	Provide physical emanations security

Design and build the TOE in such a way as to control the production of intelligible emanations within specified limits.

OT.Lifecycle_Security	Lifecycle security

The TOE shall detect flaws during the initialisation, personalisation and operational usage. The TOE shall provide safe destruction techniques for the SCD in case of re-import or re-generation.

OT.SCD_Secrecy	Secrecy of the signature-creation data

The secrecy of the SCD (used for signature generation) is reasonably assured against attacks with a high attack potential.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

OT.SCD_SVD_Corresp	Correspondence between SVD and SCD

The TOE shall ensure the correspondence between the SVD and the SCD. The TOE shall verify on demand the correspondence between the SCD stored in the TOE and the SVD if it has been sent to the TOE.

OT.SVD_Auth_TOE	TOE ensures authenticity of the SVD

The TOE provides means to enable the CGA to verify the authenticity SVD that has been exported by that TOE.

OT.Tamper_ID	Tamper detection

The TOE provides system features that detect physical tampering of a system component, and use those features to limit security breaches.

OT.Tamper_Resistance	Tamper resistance

The TOE prevents or resists physical tampering with specified system devices and components.

OT.Init	SCD/SVD generation

The TOE provides security features to ensure that the generation of the SCD and the SVD is invoked by authorized users only.

OT.SCD_Unique	Uniqueness of the signature-creation data

The TOE shall ensure the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. The SCD used for signature generation can practically occur only once and cannot be reconstructed from the SVD. In that context 'practically occur once' means that the probability of equal SCDs is negligible low.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

OT.SCD_Transfer	Secure transfer of SCD between SSCD

The TOE shall ensure the confidentiality of the SCD transferred between SSCDs.

OT.DTBS_Integrity_TOE	Verification of the DTBS-representation integrity

The TOE shall verify that the DTBS-representation received from the SCA has not been altered in transit between the SCA and the TOE. The TOE itself shall ensure that the DTBS representation is not altered by the TOE as well. Note, that this does not conflict with the signature-creation process where the DTBS itself could be hashed by the TOE.

OT.Sigy_SigF	Signature generation function for the legitimate signatory only

The TOE provides the signature generation function for the legitimate signatory only and protects the SCD against the use of others. The TOE shall resist attacks with high attack potential.

OT.Sig_Secure	Cryptographic security of the electronic signature

The TOE generates electronic signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD cannot be reconstructed using the electronic signatures. The electronic signatures shall be resistant against these attacks, even when executed with a high attack potential.

4.7.2 Complementary security objectives of the TOE

OT.Authentication_Secure	Secure authentication mechanisms

The TOE provides strong mechanism to authenticate external users/entity and mechanisms to establish a strong trusted channel wit ha remote IT entity. The authentication protocols rely on cryptographic schemes that are based on either symmetric or asymmetric cryptography. The TOE uses freshly generated random number in the authentication mechanism in order to avoid replay attacks. The authentication protocols ensure that the cryptogram can not be forged without the knowledge of the authentication key, and that they can not be reconstructed from the authentication cryptograms. The trusted channel ensures integrity, authenticity, and confidentiality of the data using strong encryption techniques. The trusted channel ensures protection against deletion, and modification of commands. Moreover the TOE ensures the key its uses are genuine by

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

enforcing an access control over the authentication keys update, in order to ensure that only entitled entities can change key values.

OT.SCD/SVD_Management	Management of SCD/SVD

The TOE enables to manage SCD/SVD. Each key (pair) and RAD may be created at any time and used to perform qualified signature during the TOE life time. Several SCD, SVD, and RAD may be present on the TOE and used by the same holder. The TOE guarantees the SCD, SVD and RAD are independent from each other.

OT.Key_Lifecycle_Security	Lifecycle security of the key(s) stored in the TOE

The TOE shall detect flaws during the initialisation, personalisation and operational usage. The TOE shall provide safe destruction techniques for the authentication keys (of the TOE and/or the external entities) and eServices keys it stores in case of erasure, re-import or re-generation.

OT.Key_Secrecy	Secrecy of the key(s) stored in the TOE

The secrecy of the authentication keys (of the TOE and/or the external entities) and eServices keys stored in the TOE is reasonably assured against attacks with a high attack potential.

OT.TOE_AuthKey_Unique	Uniqueness of the TOE authentication key(s)

The TOE shall ensure the cryptographic quality of the asymmetric authentication key pair used for the TOE authentication. The private key used for TOE authentication can practically occur only once and cannot be reconstructed from the public key. In that context 'practically occur once' means that the probability of equal TOE authentication key is negligible low.

OT.LifeCycle_Management	Management of the life cycle

The TOE provides a life cycle management enabling to separate its life cycle in two main phases.

The first one (phase 6) is the one during the TOE is under the sole control of the Personalization Agent. The following operation may be realized:

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

- The **SCD**, **SVD** and keys may be created, generated, imported or erased
- The **RAD** (s) may be created and loaded
- **SVD** and public keys may be exported

Once performed, the Personalisation Agent switches the TOE in phase 7. This transition is irreversible leaving the TOE under the sole control of the signatory, the administrator (including the SCA, CGA, SSCD, IFD) and the TOE_Administrator according to the security rules set by the Personalisation Agent.

OT.eServices	**Provision of eServices**

The TOE provides eServices Mechanisms enabling to:

- decrypt encryption keys
- authenticate the TOE
- verify CVC certificates

Moreover the TOE ensures the key its uses are genuine by enforcing an access control over the keys update, in order to ensure that only entitled entities can change key values.

4.8 Security objectives for the Environment

4.8.1 Security objectives of the Environment drawn from [SSCD2] and [SSCD3]

OE.SCD_SVD_Corresp	**Correspondence between SVD and SCD**

The SSCD Type1 shall ensure the correspondence between the SVD and the SCD. The SSCD Type1 shall verify the correspondence between the SCD sent to the TOE and the SVD sent to the CGA or TOE.

OE.SCD_Transfer	**Secure transfer of SCD between SSCD**

The SSCD Type1 shall ensure the confidentiality of the SCD transferred to the TOE. The SSCD Type1 shall prevent the export of a SCD that already has been used for signature generation by the SSCD Type2. The SCD shall be deleted from the SSCD Type1 whenever it is exported into the TOE.

OE.SCD_Unique	**Uniqueness of the signature-creation data**

The SSCD Type1 shall ensure the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. The SCD used for signature generation can practically occur only once and

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

cannot be reconstructed from the SVD. In that context 'practically occur once' means that the probability of equal SCDs is negligible low.

OE.CGA_QCert	Generation of qualified certificates

The CGA generates qualified certificates which include inter alia

(a) the name of the signatory controlling the TOE,

(b) the SVD matching the SCD implemented in the TOE under sole control of the signatory,

(c) the advanced signature of the CSP.

OE.SVD_Auth_CGA	CGA verifies the authenticity of the SVD

The CGA verifies that the SSCD is the sender of the received SVD and the integrity of the received SVD. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.

OE.HI_VAD	Protection of the VAD

If an external device provides the human interface for user authentication, this device will ensure confidentiality and integrity of the VAD as needed by the authentication method employed.

OE.SCA_Data_Intend	Data intended to be signed

The SCA

(a) generates the DTBS-representation of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE,

(b) sends the DATBS-representation to the TOE and enables verification of the integrity of the DTBS-representation by the TOE

(c) attaches the signature produced by the TOE to the data or provides it separately.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

4.8.2 Complementary security objectives of the Environment

OE.LinkSCD_QualifiedCertificate	**Link between a SCD stored in the TOE and the relevant qualified certificate**

The Subject in charge of creating and updating the SCD (**Personalisation Agent**, **Administrator**, **Signatory**), or the remote IT entity involved in the updating process (the **SSCD,** the **CGA)** shall ensure an unambiguous link between the (qualified) certificate(s) and the matching SCD(s). This link might be figured out by a PKCS#15 structures, an XML structure, an identifier .linking the file containing the (qualified) certificate or the URL hosting them to the SCD(s) loaded in the TOE. In particular, it implies this link is updated, each time the SCD(s) is created, imported, erased or generated.

OE.AuthKey_Transfer	**Secure transfer of Authentication key(s) to the TOE**

The entity in charge of generating the authentication keys to be loaded in the TOE shall ensure the confidentiality of the key(s) transferred to the TOE.

OE.AuthKey_Unique	**Uniqueness of the authentication key(s)**

The entity in charge of generating the authentication keys to be loaded in the TOE shall ensure the cryptographic quality of the authentication key(s). The authentication key used for authentication can practically occur only once and, in case of a TOE authentication key cannot be reconstructed from its public portion. In that context 'practically occur once' means that the probability of equal keys is negligible low.

OE.TOE_PublicAuthKey_Transfer	**Secure transfer of Public Authentication key(s) of the TOE**

The entity in charge of generating the authentication certificate from the TOE's authentication public key generated in the TOE shall ensure the authenticity of this data when transferred from the TOE. This may be achieved by the retrieval of the public key according to certain rules imposed to the TOE holders.

OE.TOE_Construction	**Construction of the TOE by the Personalisation Agent**

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

The Personalization Agent in charge of administrating the TOE in phase 6 shall be a trusted person and shall be skilled enough to correctly apply the recommendations indicated in [**AGD_PRE**]. These recommendations are required to construct the TOE

5 Extended Requirements

5.1 Extended Families

5.1.1 Extended Family FPT_EMSEC - TOE Emanation

5.1.1.1 Family behaviour

This family defines requirements to mitigate intelligible emanations.

5.1.1.1.1 Extended Components

Extended Component FPT_EMSEC.1

Description

The family FPT_EMSEC (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE related to leakage of information based on emanation. The TOE shall prevent attacks against the TOE and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations which are not directly addressed by any other component of CC part 2 [CC31-2].

Component levelling:

Protection of the TSF and assets requires mitigate information leakage based on emanation.

Audit:

There are no actions defined to be auditable

Management:

There are no management activities foreseen

Hierarchical to:

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

No other components.

Definition

FPT_EMSEC.1 TOE Emanation

FPT_EMSEC.1.1 The TOE shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

FPT_EMSEC.1.2 The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

Dependencies: No dependencies.

5.1.2 Extended Family FCS_RNG - FCS_RNG: Random Number Generation

5.1.2.1 Family behaviour

This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.

5.1.2.1.1 Extended Components

Extended Component FCS_RNG.1

Description

A physical random number generator (RNG) produces the random number by a noise source based on physical random processes. A non-physical true RNG uses a noise source based on non-physical random processes like human interaction (key strokes, mouse movement). A deterministic RNG uses a random seed to produce a pseudorandom output. A hybrid RNG combines the principles of physical and deterministic RNGs.

Component levelling:

Generation of random numbers requires that random numbers meet a defined quality metric

Audit:

There are no actions defined to be auditable

Management:

There are no management activities foreseen

Hierarchical to:

No other components.

Definition

FCS_RNG.1 Random Number Generation

FCS_RNG.1.1 The TSF shall provide a [selection: physical, non-physical true, deterministic hybrid] random number generator that implements: [assignment: list of security capabilities].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: a defined quality metric].

Dependencies: No dependencies.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

6 Security requirements

6.1 Security Functional Requirements

6.1.1 SFR drawn from the Protection Profile

The following SFRs are drawn from [SSCD2] and [SSCD3]. They are sorted out depending on the life cycle of the TOE.

6.1.1.1 Phase 6 and 7

This chapter contains SFRs drawn for [SSCD2] and [SSCD3] that apply in both phase 6 and 7 of the life cycle.

6.1.1.1.1 FCS_CKM.1 Cryptographic key generation

FCS CKM.1.1
The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***assignment: cryptographic key generation algorithm***] and specified cryptographic key sizes [***assignment: cryptographic key sizes***] that meet the [***assignment: list of standards***]

Refinement:

cryptographic key generation algorithm	***cryptographic key sizes***	***list of standards***
RSA key generation	1024 bits or 1536 bits or 2048 bits	[ANSIX9.31]
Key pair over Elliptic curve	Any elliptic curve from 160 bits up to 521 bits with prime field p	[IEEE]

6.1.1.1.2 FCS_CKM.4 Cryptographic key destruction

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FCS_CKM.4.1 / SCD/SVD

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [***overwriting the buffer containing the key with zero***] that meets the following: [***none***].

Refinement:
This SFR applies to all keys, whether it is the SCD, the SVD or another one.

Application note:
The cryptographic key SCD will be destroyed on demand of the Signatory or Administrator. The destruction of the SCD is mandatory before the SCD is re-imported into the TOE.

6.1.1.1.3 FDP_ACC Access Control Policy

FDP_ACC.1.1/SVD transfer SFP

The TSF shall enforce the [***SVD transfer SFP***] on [***import and export of SVD by User***].

FDP_ACC.1.1/Initialisation SFP

The TSF shall enforce the [***Initialisation SFP***] on [***Generation of SCD/SVD pair by User***].

FDP_ACC.1.1/ Personalisation SFP

The TSF shall enforce the [***Personalisation SFP***] on [***Creation of PIN RAD by Administrator***].

FDP_ACC.1.1/SCD Import SFP

The TSF shall enforce the [***SCD Import SFP***] on [***Import or erasure of SCD by User***].

6.1.1.1.4 FDP_ACF Security attribute based access control

For the definition of the attribute, refer to Annex A : Attributes for FDP_ACF Security attribute based access control

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

6.1.1.1.4.1SVD transfer SFP

FDP_ACF.1.1/ SVD transfer SFP
The TSF shall enforce the [***SVD transfer SFP***] to objects based on [***General attribute***]

FDP_ACF.1.2/ SVD transfer SFP
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:***[the user with the security attribute "role" set to "Administrator" or "Signatory" is allowed to export SVD]***

Refinement:
In phase 6, the entity with the role "Administrator" is the "Personalisation Agent" and always has the security attribute "SCD/SVD Management" set to "authorized".
In phase 7, depending on the use case, the role allowed to export the SVD may be restricted to "Administrator", one of its sub role ("Personalisation Agent", "SCA", "CGA", SSCD type 1", "IFD", "User_Admin"), to "Signatory" or any combination of them.

FDP_ACF.1.3/ SVD transfer SFP
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***none***]

FDP_ACF.1.4/ SVD transfer SFP
The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [***none***]

6.1.1.1.4.2 Initialisation SFP

FDP_ACF.1.1/ Initialisation SFP
The TSF shall enforce the [***Initialisation SFP***] to objects based on [***General attribute***] and [***Initialisation attribute group***].

FDP_ACF.1.2/ Initialisation SFP
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:***[the user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD/SVD management" set to "authorised" is allowed to generate SCD/SVD pair.***]

Refinement:
In phase 6, the entity with the role "Administrator" is the «Personalisation Agent» and always has the security attribute "SCD/SVD Management" set to "authorized".
In phase 7, depending on the use case, the role allowed to export the SVD may be restricted to "Administrator", one of its sub role ("Personalisation Agent", "SCA", "CGA", SSCD type 1", "IFD", "User_Admin"), to "Signatory" or any combination of them.

FDP_ACF.1.3/ Initialisation SFP
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***none***]

FDP_ACF.1.4/ Initialisation SFP

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:[***the user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD/SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair.***]

Refinement:

In phase 6, the entity with the role “Administrator” is the «Personalisation Agent» and always has the security attribute “SCD/SVD Management” set to “authorized”.

6.1.1.1.4.3 SCD Import SFP

FDP_ACF.1.1/ SCD Import SFP

The TSF shall enforce the [***SCD Import SFP***] to objects based on [***General attribute***] and [***Initialisation attribute group***].

FDP_ACF.1.2/ SCD Import SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***[the user with the security attribute "role" set to "Administrator" or set to "Signatory" and with the security attribute "SCD/SVD management" set to "authorised" is allowed to import SCD if the security attribute "secure SCD import allowed" is set to "yes".]***

Refinement:

In phase 6, the entity with the role “Administrator” is the «Personalisation Agent» and always has the security attribute “SCD/SVD Management” set to “authorized” and “secure SCD import allowed” set to Yes.

In phase 7, depending on the use case, the role allowed to export the SVD may be restricted to “Administrator”, one of its sub role (“Personalisation Agent”, “SCA”, “CGA”, SSCD type 1”, “IFD”, “User_Admin”), to “Signatory” or any combination of them.

FDP_ACF.1.3/ SCD Import SFP

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***none***]

FDP_ACF.1.4/ SCD Import SFP

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

(a) [***the user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD/SVD management" set to "not authorised" is not allowed to import SCD if the security attribute "secure SCD import allowed" is set to "yes".***]

(b) [***the user with the security attribute "role" set to "Administrator" or to "Signatory" and with the security attribute "SCD/SVD management" set to "authorised" is not allowed to import SCD if the security attribute "secure SCD import allowed" is set to "no".***]

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d’Estienne d’Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

6.1.1.1.4.4 Personalisation SFP

FDP_ACF.1.1/ Personalisation SFP The TSF shall enforce the [***Personalisation SFP***] to objects based on Personalisation SFP [***General attribute group***]

FDP_ACF.1.2/ Personalisation SFP The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [***user with the security attribute "role" set to "Administrator" is allowed to create the RAD***]

Refinement:
In phase 6, the entity with the role “Administrator” is the «Personalisation Agent».
In phase 7, depending on the use case, the role allowed to export the SVD may be restricted to “Administrator”, one of its sub role (“Personalisation Agent”, “SCA”, “CGA”, SSCD type 1”, “IFD”, “User_Admin”), to “Signatory” or any combination of them.

FDP_ACF.1.3/ Personalisation SFP The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***none***]

FDP_ACF.1.4/ Personalisation SFP The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [***none***]

6.1.1.1.5 FDP_ETC : Export to outside TSF control

6.1.1.1.5.1 SVD Transfer

FDP_ETC.1.1/ SVD transfer The TSF shall enforce the [***SVD transfer SFP***] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2/ SVD transfer The TSF shall export the user data without the user data's associated security attributes.

6.1.1.1.6 FDP_ITC Import from outside TSF control

6.1.1.1.6.1 SCD Import

FDP_ITC.1.1/ SCD The TSF shall enforce the [***SCD Import SFP***] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/ SCD The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d’Estienne d’Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FDP_ITC.1.3/ SCD
The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [***SCD shall be sent by an Authorised SSCD***].

Application note:
A SSCD of Type 1 is authorized to send SCD to a SSCD of Type 2, if it is designated to generate the SCD for this SSCD of Type 2 and to export the SCD for import into this SSCD of Type 2. Authorized SSCD of Type 1 is able to establish a trusted channel to the SSCD of Type 2 for SCD transfer as required by FTP_ITC.1.3/SCD export.
In phase 6, the authorized SSCD is the «Personalisation Agent» that has the role "Administrator".

6.1.1.1.7 FDP_RIP Residual information protection

FDP_RIP.1.1
The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***de-allocation of the resource from***] the following objects: [***secure messaging data (session keys and SSC), keys, SCD, VAD, and RAD***].

6.1.1.1.8 FDP_SDI Stored data integrity

6.1.1.1.8.1 Persistent data

The following data persistently stored by TOE have the user data attribute "integrity checked persistent stored data"

- SCD
- RAD
- SVD
- Keys
- Diffie Hellman domain parameters

FDP_SDI.2.1/ Persistent
The TSF shall monitor user data stored in containers controlled by the TSF for [***integrity error***] on all objects, based on the following attributes: [***integrity checked persistent stored data***].

FDP_SDI.2.2/ Persistent
Upon detection of a data integrity error, the TSF shall:
[***1. prohibit the use of the altered data***
2. inform the Signatory about integrity error.]

6.1.1.1.9 FDP_UCT Inter-TSF user data confidentiality transfer protection

6.1.1.1.9.1 SCD Import

FDP_UCT.1.1/ Receiver
The TSF shall enforce the [***SCD Import SFP***] to [***receive***] user data in a manner protected from unauthorised disclosure.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

6.1.1.1.10 FDP_UIT Inter-TSF user data integrity transfer protection

6.1.1.1.10.1 SVD transfer

FDP_UIT.1.1/ SVD transfer The TSF shall enforce the [***SVD transfer SFP***] to [***transmit***] user data in a manner protected from [***modification and insertion***] errors.

FDP_UIT.1.2/ SVD transfer The TSF shall be able to determine on receipt of user data, whether [***modification and insertion***] has occurred.

6.1.1.1.11 FIA_UAU User authentication

FIA UAU.1.1 The TSF shall allow [***Identification of the user by means of TSF required by FIA_UID.1***] [***Establishing a trusted channel between the TOE and a SSCD of type 1 by means of TSF required by FTP_ITC.1/SCD import***] [***Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE to transmit the VAD***] [***Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import in phase 7***] On behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note:
"Local user" mentioned in component FIA_UAU.1.1 is the user using the trusted path provided between the SCA in the TOE environment and the TOE as indicated by FTP_TRP.1/SCA and FTP TRP.1/TOE.
This trusted path enables to authenticate the role Signatory and Administrator (if it is authenticated with a RAD).

6.1.1.1.12 FIA_UID User Identification

FIA UID.1.1 The TSF shall allow [***Establishing a trusted channel between the TOE and a SSCD of type 1 by means of TSF required by FTP_ITC.1/SCD import***] [***Establishing a trusted path between local user and the TOE by means of TSF required by FTP_TRP.1/TOE to transmit the VAD***] [***Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS import in phase 7***] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.1.1.13 FMT_MSA Management of security attributes

FMT_MSA.1.1/ Administrator - Initialisation
The TSF shall enforce the [***Initialisation SFP***] to restrict the ability to [***modify***] the security attributes [***SCD/SVD management***] to [***Administrator***].

FMT_MSA.1.1/ Administrator - Import
The TSF shall enforce the [***SCD Import SFP***] to restrict the ability to [***modify***] the security attributes [***SCD/SVD management and secure SCD import allowed***] to [***Administrator***].

FMT_MSA.2.1
The TSF shall ensure that only secure values are accepted for [***SCD/SVD management, SCD operational, Medium, HashOffCard, SymAuthMechanism, AsymAuthMechanism, Key import management, Key generation management, Key export Management]***.

FMT_MSA.3.1
The TSF shall enforce the [***Initialisation SFP, Signature-creation SFP, SCD Import SFP, IAS ECC Administration SFP, Key Management SFP***] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

Refinement:
The security attribute of the SCD "SCD operational" is set to "no" after generation or import of the SCD.

FMT_MSA.3.2
The TSF shall allow the [***assignment : the authorised identified role***] to specify alternative initial values to override the default values when an object or information is created.

Refinement:
The following refinement applies:

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

Security attributes	*phases*	*Authorized identified role*
SCD/SVD Management	6&7	Administrator
SCD Operational	7	Administrator
Medium HashOffCard SymAuthMechanism AsymAuthMechanism	6	Personalisation Agent
Medium HashOffCard SymAuthMechanism AsymAuthMechanism	7	TOE_Administrator
Key import Management Key generation Management Key export Management	6	Personalisation Agent
Key import Management Key generation Management Key export Management	7	Signatory, User_Admin, SCA, CGA, SSCD type 1, IFD
Secure SCD import Allowed	6	Personalisation Agent
Secure SCD import Allowed	7	SSCD type 1
Sent by an authorized SCA	7	SCA

6.1.1.1.14 FMT_SMR Security management roles

FMT_SMR.1.1
The TSF shall maintain the roles ["***User_Admin", "Signatory", "SCA", "CGA", "SSCD", "Personalisation Agent", "IFD" and "TOE_Administrator"***].

FMT_SMR.1.2
The TSF shall be able to associate users with roles.

Application note:
The role "Administrator" is equivalent to one of the following roles: "User_Admin", "Personalisation Agent", and depending on the configuration of the TOE, to "SCA", "CGA", "SSCD".

6.1.1.1.15 FPT_EMSEC TOE Emanation

FPT_EMSEC.1.1
The TOE shall not emit [***Side channel emission***] in excess of [***limits specified by the state-of-the-art attacks on smart card IC***] enabling access to [***RAD, SCD, keys and TSF data***] and [***none***].

FPT_EMSEC.1.2

The TSF shall ensure [***all users***] are unable to use the following interface [***external contacts emanations***] to gain access to [***RAD, SCD, keys and TSF data***] and [***none***].

6.1.1.1.16 FPT_FLS Failure secure

FPT_FLS.1.1
The TSF shall preserve a secure state when the following types of failures occur: [
Card reset or tearing,
Security violation detected by [PLT] with FAU_ARP.1,
Failure detected by [PLT] with FPT_FLS.1, FPT_FLS.1/ADEL, FPT_FLS.1/ODEL, and FPT_FLS.1/SCP
Integrity error detected on RAD, SCD, and keys].

6.1.1.1.17 FPT_PHP TSF physical Protection

FPT_PHP.1.1
The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2
The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.3.1
The TSF shall resist [***physical manipulation and physical probing***] to the [***all TOE components implementing the TSF***] by responding automatically such that the SFRs are always enforced

6.1.1.1.18 FPT_TST TSF self test

FPT_TST.1.1
The TSF shall run a suite of self-tests [***during initial start-up and periodically during normal operation***] to demonstrate the correct operation of [***the TSF***].

FPT_TST.1.2
The TSF shall provide authorised users with the capability to verify the integrity of [***TSF data***].

FPT_TST.1.3
The TSF shall provide authorised users with the capability to verify the integrity of [***TSF executable code***].

6.1.1.1.19 FTP_ITC Inter-TSF trusted channel

6.1.1.1.19.1 SCD Import

FTP_ITC.1.1/ SCD import

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/ SCD import
The TSF shall permit [***another trusted IT product***] to initiate communication via the trusted channel.

FTP_ITC.1.3/ SCD import
The TSF shall initiate communication via the trusted channel for [***SCD import***]

6.1.1.1.19.2 SVD Transfer

FTP_ITC.1.1/ SVD transfer
The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/ SVD transfer
The TSF shall permit [***another trusted IT product***] to initiate communication via the trusted channel.

FTP_ITC.1.3/ SVD transfer
The TSF shall initiate communication via the trusted channel for [***SVD transfer***]

Refinement:
The mentioned remote trusted IT product is a SSCD of type 1.for SVD import and the CGA for the SVD export.

Application note:
FTP_ITC.1/SVD Transfer will be required only, if the TOE is to import the SVD from a SSCD Type1 so it will be exported to the CGA for certification.

6.1.1.1.20 FTP_TRP Trusted path

FTP_TRP.1.1/ TOE
The TSF shall provide a communication path between itself and [***local***] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [***modification or disclosure***].

FTP_TRP.1.2/ TOE
The TSF shall permit [***local users***] to initiate communication via the trusted path.

FTP_TRP.1.3/ TOE
The TSF shall require the use of the trusted path for [***initial user authentication***].

6.1.1.2 Phase 7

This chapter contains SFRs drawn for [SSCD2] and [SSCD3] that apply in 7 of the life cycle.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

6.1.1.2.1 FCS_COP Cryptographic operation

FCS_COP.1.1/ CORRESP
The TSF shall perform [***SCD/SVD correspondence verification***] in accordance with a specified cryptographic algorithm [***assignment : cryptographic algorithm***] and cryptographic key sizes [***assignment : cryptographic key sizes***] that meet the following: [***assignment : list of standards***].

Refinement:

cryptographic algorithm	*cryptographic key sizes*	*list of standards*
PKCS #1 V1.5 Block Type 1 with Message Digest Info with RSA CRT and hashing algorithm SHA-1 or SHA-256	1024 bits or 1536 bits or 2048 bits	[PKCS#1]
ECDSA-SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	Any elliptic curve from 160 bits up to 521 bits with prime field p	[ANSIX9.62]

FCS_COP.1.1/ SIGNING
The TSF shall perform [***Digital signature-generation***] in accordance with a specified cryptographic algorithm [***assignment : cryptographic algorithm***] and cryptographic key sizes [***assignment : cryptographic key sizes***] that meet the following: [***assignment : list of standards***].

Refinement:

cryptographic algorithm	*cryptographic key sizes*	*list of standards*
PKCS #1 V1.5 Block Type 1 with Message Digest Info with RSA CRT and hashing algorithm SHA-1 or SHA-256	1024 bits or 1536 bits or 2048 bits	[PKCS#1]
ECDSA-SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	Any elliptic curve from 160 bits up to 521 bits with prime field p	[ANSIX9.62]

6.1.1.2.2 FDP_ACC Access Control Policy

FDP_ACC.1.1/Signature-creation SFP
The TSF shall enforce the [***Signature-creation SFP***] on

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

[***Sending of DTBS representation by SCA***]
[***Signing of DTBS-representation by Signatory***].

6.1.1.2.3 FDP_ACF Security attribute based access control

For the definition of the attribute, refer to Annex A : Attributes for FDP_ACF Security attribute based access control.

6.1.1.2.3.1 Signature Creation SFP

FDP_ACF.1.1/ Signature-creation SFP
The TSF shall enforce the [***Signature-creation SFP***] to objects based on [***General attribute group***] and [***Signature-creation attribute group***].

FDP_ACF.1.2/ Signature-creation SFP
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
[***User with the security attribute "role" set to "Signatory" is allowed to create electronic signatures for DTBS sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "yes"***]

FDP ACF.1.3/ Signature-creation SFP
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***none***]

FDP_ACF.1.4/ Signature-creation SFP
The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
(a) [***User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures for DTBS which is not sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "yes".]***
(b) [***User with the security attribute "role" set to "Signatory" is not allowed to create electronic signatures for DTBS sent by an authorized SCA with SCD by the Signatory which security attribute "SCD operational" is set to "no".]***

6.1.1.2.4 FDP_ITC Import from outside TSF control

6.1.1.2.4.1 DTBS import

FDP_ITC.1.1/ DTBS
The TSF shall enforce the [***Signature-creation SFP***] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/ DTBS
The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/ DTBS

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [***DTBS-representation shall be sent by an Authorised SCA***].

Application note:
A SCA is authorized to send the DTBS-representation if it is actually used by the Signatory to create an electronic signature and able to establish a trusted channel to the SSCD as required by FTP_ITC.1.3/SCA DTBS.

6.1.1.2.5 FDP_SDI Stored data integrity

6.1.1.2.5.1 DTBS-representation

The Protection Profiles [SSCD2] and [SSCD3] specify that the DTBS representation temporarily stored by TOE have the user data attribute "integrity checked stored data".

FDP_SDI.2.1/ DTBS
The TSF shall monitor user data stored in containers controlled by the TSF for [***integrity error***] on all objects, based on the following attributes: [***integrity checked stored data***].

FDP_SDI.2.2/ DTBS
Upon detection of a data integrity error, the TSF shall:
[***1. prohibit the use of the altered data***
2. inform the Signatory about integrity error.]

6.1.1.2.6 FDP_UIT Inter-TSF user data integrity transfer protection

6.1.1.2.6.1 DTBS transfer

FDP_UIT.1.1/ TOE DTBS
The TSF shall enforce the [***Signature-creation SFP***] to [***receive***] user data in a manner protected from [***modification, deletion and insertion***] errors.

FDP_UIT.1.2/ TOE DTBS
The TSF shall be able to determine on receipt of user data, whether [***modification, deletion and insertion***] has occurred.

6.1.1.2.7 FIA_AFL Authentication failure

FIA AFL.1.1/RAD
The TSF shall detect when [***an administrative configurable positive integer within 1 and 15***] unsuccessful authentication attempts occur related to [***consecutive failed authentication attempts***].

FIA AFL.1.2/RAD
When the defined number of unsuccessful authentication attempts has been [***met or surpassed***], the TSF shall [***block RAD***].

Application note:
These SFRs apply to the users Signatory and Administrator, if the latter uses a RAD to authenticate itself.

6.1.1.2.8 FIA_ATD User attribute definition

FIA ATD.1.1 / S.Signatory The TSF shall maintain the following list of security attributes belonging to individual users [***RAD***]

FIA ATD.1.1 / S.Admin The TSF shall maintain the following list of security attributes belonging to individual users [***RAD***]

Application Note:
This SFR applies when the user "Administrator" is authenticated by mean of a RAD.

6.1.1.2.9 FMT_MSA Management of security attributes

FMT_MSA.1.1/ Signatory The TSF shall enforce the [***Signature-creation SFP***] to restrict the ability to [***modify***] the security attributes [***SCD operational***] to [***Signatory***].

6.1.1.2.10 FMT_MTD Management of TSF data

6.1.1.2.10.1 Signatory

FMT_MTD.1.1/ Signatory The TSF shall restrict the ability to [***modify***] the [***RAD***] to [***Signatory***].

Refinement:
This requirement applies only if the RAD belonging to the user Signatory.

6.1.1.2.11 FMT_MOF Management of functions in TSF

FMT_MOF.1.1 The TSF shall restrict the ability to [***enable***] the functions [***signature-creation function***] to [***Signatory***].

6.1.1.2.12 FTP_ITC Inter-TSF trusted channel

6.1.1.2.12.1 DTBS Import

FTP_ITC.1.1/ DTBS import The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/ DTBS import The TSF shall permit [***another trusted IT product***] to initiate communication via the trusted channel.

FTP_ITC.1.3 DTBS import

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

The TSF shall initiate communication via the trusted channel for [***signing DTBS-representation***]

Refinement:
The mentioned remote trusted IT product is a SCA.

6.1.2 Additional SFRs

6.1.2.1 Phase 6

6.1.2.1.1 FCS_COP Cryptographic operation

FCS_COP.1.1/ GP secret data protection The TSF shall perform [***GP secret data encryption***] in accordance with a specified cryptographic algorithm [***assignment: cryptographic algorithm***] and cryptographic key sizes [***assignment: cryptographic key size***] that meet the following: [***assignment: list of standards***].

Refinement:

cryptographic algorithm	*cryptographic key sizes*	*list of standards*
SCP02 using Triple DES	128 bits	[GP2.1.1]
SCP03 using AES	128, 192 and 256 bits	[SCP03]
Proprietary SCP03 using AES	128, 192 and 256 bits	[PLT]

Application Note:

The type of algorithm used by the TOE depends on the configuration set during the javacard open platform personalisation (For more details see [AGD_PRE_PLT]).

6.1.2.1.2 FMT_MTD Management of TSF data

6.1.2.1.2.1 TOE Serial number

FMT_MTD.1.1/ TOE Serial number The TSF shall restrict the ability to [***set***] the [***Serial number of the TOE***] to [***Personalisation Agent***].

6.1.2.1.2.2 TOE State

FMT_MTD.1.1/ TOE State

The TSF shall restrict the ability to [***switch***] the [***TOE from phase 6 to phase 7***] to [***Personalisation Agent***].

6.1.2.2 Phase 7

6.1.2.2.1 FCS_CKM.1 Cryptographic key generation

FCS CKM.1.1 / Session keys The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***assignment : cryptographic algorithm***] and specified cryptographic key sizes [***assignment : cryptographic key sizes***] that meet the [***assignment : list of standards***]

Refinement:

cryptographic algorithm	*cryptographic key sizes*	*list of standards*
Key Derivation function	DES keys of 128 bits	[14890]
Key Derivation function	Two AES keys of 128, 192 and 256 bits	[14890]
Key Derivation function	Three AES keys of 128, 192 and 256 bits	[14890]

6.1.2.2.2 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 / Session keys The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [***overwriting the buffer containing the key with zero***] that meets the following: [***none***].

6.1.2.2.3 FCS_COP Cryptographic operation

FCS_COP.1.1/ Diffie Hellman computation The TSF shall perform [***Key Agreement***] in accordance with a specified cryptographic algorithm [***Diffie Hellmann***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***PKCS#3***].

FCS_COP.1.1/ Secure Messaging in Confidentiality

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

The TSF shall perform [***Secure Messaging in confidentiality***] in accordance with a specified cryptographic algorithm [***assignment: cryptographic algorithm***] and cryptographic key sizes [***assignment: cryptographic key sizes***] that meet the following: [***assignment: list of standards***].

Refinement:

cryptographic algorithm	*cryptographic key sizes*	*list of standards*
Encryption with Triple DES EDE in CBC mode	128 bits	[11568-2]
Encryption with AES in CBC mode	128, 192 and 256 bits	[11568-2]

Application Note: This algorithm is used during secure Messaging to ensure confidentiality of incoming and outgoing data.

FCS_COP.1.1/ Secure Messaging in Integrity

The TSF shall perform [***Secure Messaging in integrity and authenticity***] in accordance with a specified cryptographic algorithm [***assignment: cryptographic algorithm***] and cryptographic key sizes [***assignment: cryptographic key sizes***] that meet the following: [***assignment: list of standards***].

Refinement:

cryptographic algorithm	*cryptographic key sizes*	*list of standards*
Retail MAC MAC algorithm 3 with padding method 2 and DES bloc Cipher	128 bits	[9797-1]
EMAC MAC algorithm 2 with padding method 2 and AES bloc Cipher with a length of eight bytes	128, 192 and 256 bits	[9797-1]
CMAC CMAC with pre padding method 2 and AES bloc Cipher with a	128, 192 and 256 bits	[SP800-38B]

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

length of eight bytes		

Application Note: This algorithm is used during secure Messaging to ensure integrity and authenticity of incoming and outgoing data.

FCS_COP.1.1/ C/S Authentication

The TSF shall perform [***Client/Server Authentication***] in accordance with a specified cryptographic algorithm [***raw ECDSA***] and cryptographic key sizes [***Any elliptic curve from 160 bits up to 521 bits with prime field p***] that meet the following: [***ANSIX9.62***].

FCS_COP.1.1/ Encryption key decipherment

The TSF shall perform [***Encryption key decipherment***] in accordance with a specified cryptographic algorithm [***Diffie Hellman on an Elliptic curve***] and cryptographic key sizes [***Any elliptic curve from 160 bits up to 521 bits with prime field p***] that meet the following: [***TR03111***].

FCS_COP.1.1/ Symmetric Role Authentication

The TSF shall perform [***Symmetric Role Authentication***] in accordance with a specified cryptographic algorithm [***assignment: cryptographic algorithm***] and cryptographic key sizes [***assignment: cryptographic algorithm***] that meet the following: [***assignment: list of standards***].

Refinement:

cryptographic algorithm	***cryptographic key sizes***	***list of standards***
Encryption using Triple DES EDE in mode CBC Signature using Retail MAC	128 bits	[IASECC]
Encryption using AES in mode CBC Signature using EMAC	128, 192 and 256 bits	[14890]
Encryption using AES in mode CBC Signature using CMAC	128, 192 and 256 bits	[14890]
Encryption using Triple DES EDE in mode CBC	128 bits	[Minidriver]

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FCS_COP.1.1/ Symmetric Device Authentication

The TSF shall perform [***Symmetric Device Authentication***] in accordance with a specified cryptographic algorithm [***assignment: cryptographic algorithm***] and cryptographic key sizes [***assignment: cryptographic algorithm***] that meet the following: [***assignment : list of standards***].

Refinement:

cryptographic algorithm	***cryptographic key sizes***	***list of standards***
Encryption using Triple DES EDE in mode CBC Signature using Retail MAC	128 bits	[IASECC]
Encryption using AES in mode CBC Signature using EMAC	128, 192 and 256 bits	[14890]
Encryption using AES in mode CBC Signature using CMAC	128, 192 and 256 bits	[14890]

FCS_COP.1.1/ Certificate Verification

The TSF shall perform [***Certificate verification***] in accordance with a specified cryptographic algorithm [***RSA with ISO/IEC 9796-2 padding with partial recovery and with SHA-1 or SHA-256***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***IASECC***].

FCS_COP.1.1/ Asymmetric Role Authentication

The TSF shall perform [***Asymmetric Role Authentication***] in accordance with a specified cryptographic algorithm [***RSA with ISO/IEC 9796-2 padding with partial recovery and with SHA-1 or SHA-256***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***IASECC***].

FCS_COP.1.1/ Asymmetric Internal DAPP Authentication

The TSF shall perform [***Asymmetric Internal DAPP Authentication***] in accordance with a specified cryptographic algorithm [***RSA with ISO/IEC 9796-2 padding with partial recovery and with SHA-1 or SHA-256***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***IASECC***].

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FCS_COP.1.1/ Asymmetric External DAPP Authentication

The TSF shall perform [***Asymmetric External DAPP Authentication***] in accordance with a specified cryptographic algorithm [***RSA with ISO/IEC 9796-2 padding with partial recovery and with SHA-1 or SHA-256***] and cryptographic key sizes [***1024 bits, 1536 bits or 2048 bits***] that meet the following: [***IASECC***].

6.1.2.2.4 FMT_MTD Management of TSF data

6.1.2.2.4.1 Association between SCD and SCD_ID

FMT_MTD.1.1/ Association between SCD and SCD_ID
The TSF shall restrict the ability to [***select***] the [***SCD using a SCD_ID***] to [***Any User***].

Application note:
At creation, the SCD is given a SCD identifier that will be permanently associated to it and used by the TOE to select it.

6.1.2.2.4.2 Unblocking of RAD

FMT_MTD.1.1/ Unblock
The TSF shall restrict the ability to [***unblock***] the [***RAD***] to [***Administrator***].

Application note:
This SFR apply to any RAD (belonging to Signatory or Administrator).

6.1.2.3 Phase 6&7

6.1.2.3.1 FCS_COP Cryptographic operation

FCS_COP.1.1/ Data hashing

The TSF shall perform [***data hashing***] in accordance with a specified cryptographic algorithm [***SHA-1, partial SHA-1, SHA-224, SHA-256, partial SHA-256, SHA-384, and SHA-512***] and cryptographic key sizes [***none***] that meet the following: [***FIPS 180-3***].

FCS_COP.1.1/ GP Authentication

The TSF shall perform [***Mutual Authentication***] in accordance with a specified cryptographic algorithm [***assignment: cryptographic algorithm***] and cryptographic key sizes [***assignment: cryptographic key sizes***] that meet the following: [***assignment: list of standards***].

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

Refinement:

cryptographic algorithm	*cryptographic key sizes*	*list of standards*
SCP02 using Triple DES	128 bits	[GP2.1.1]
SCP03 using AES	128, 192 and 256 bits	[SCP03]
Proprietary SCP03 using AES	128, 192 and 256 bits	[PLT]

Application Note:

The type of algorithm used by the TOE depends on the configuration set during the javacard open platform personalisation (For more details see [AGD_PRE_PLT]).

6.1.2.3.2 FCS_RNG Random Number Generation

FCS_RNG.1 / Random Number Generation

FCS_RNG.1.1
The TSF shall provide a [***hybrid***] random number generator that implements: [***none***].

FCS_RNG.1.2
The TSF shall provide random numbers that meet [***RGS_B1***].

6.1.2.3.3 FDP_ACC Access Control Policy

FDP_ACC.1.1/IAS ECC Administration SFP

The TSF shall enforce the [***IAS ECC Administration SFP***] on [***Management of Medium, HashOffCard, SymAuthMechanisms and AsymAuthMechanisms by the TOE Administrator (in phase 7) or Personalisation Agent (in phase 6)***].

FDP_ACC.1.1/Key Management SFP

The TSF shall enforce the [***Key Management SFP***] on
(a) [***Import of key and Diffie Hellman Domain parameters by the User***]
(b) [***Generation of asymmetric key pair by the User***]

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

(c) [***Export of public key and Diffie Hellman Domain parameters by the User***].

Application note:
This SFP applies to the all the Diffie Hellman Domain parameters and keys handled by the TOE other than the SCD and SVD.

6.1.2.3.4 FDP_ACF Security attribute based access control

For the definition of the attribute, refer to Annex A : Attributes for FDP_ACF Security attribute based access control.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

6.1.2.3.4.1 IAS ECC Administration SFP

FDP_ACF.1.1/ IAS ECC Administration SFP
The TSF shall enforce the [***IAS ECC Administration SFP***] to objects based on [***Administration group***].

FDP_ACF.1.2/ IAS ECC Administration SFP
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

(a) [***In phase 6, subject with the security attribute "role" set to "Personalisation Agent" is allowed to modify the TOE attributes***]

(b) [***In phase 7, subject with the security attribute "role" set to "TOE_Administrator" is allowed to modify the TOE attributes***]

FDP ACF.1.3/ IAS ECC Administration SFP
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***none***]

FDP_ACF.1.4/ IAS ECC Administration SFP
The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

(a) [***In phase 6, subject without the security attribute "role" set to "Personalisation Agent" is allowed to modify the TOE attributes***]

(b) [***In phase 7, subject without the security attribute "role" set to "TOE_Administrator" is allowed to modify the TOE attributes***]

6.1.2.3.4.2 Key Management SFP

FDP_ACF.1.1/ Key Management SFP
The TSF shall enforce the [***Key Management SFP***] to objects based on [***Key Management group***].

FDP_ACF.1.2/ Key Management SFP
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

(a) [***In phase 7, the user with the security attribute "role" set to "Signatory", "User_Admin", "SCA", CGA", "IFD" or "SSCD type 1" and with the security attribute "Key import Management" set to "authorised" is allowed to import key and Diffie Hellman Domain parameters]***

(b) [***In phase 6, the user with the security attribute "role" set to "Personalisation Agent" is allowed to import key and Diffie Hellman Domain parameters***]

(c) [***In phase 7, the user with the security attribute "role" set to "Signatory", "User_Admin", "SCA", CGA", "IFD" or "SSCD type 1" and with the security attribute "Key generation Management" set to "authorised" is allowed to generate a key pair***]

(d) [***In phase 6, the user with the security attribute "role" set to "Personalisation Agent" is allowed to generate a key pair***]

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

(e) [***In phase 7, the user with the security attribute "role" set to "Signatory", "User_Admin", "SCA", CGA", "IFD" or "SSCD type 1" and with the security attribute "Key export Management" set to "authorised" is allowed to export a public key and Diffie Hellman Domain parameters***]

(f) [***In phase 6, the user with the security attribute "role" set to "Personalisation Agent" is allowed to export a public key and Diffie Hellman Domain parameters***]

(g) [***In phase 7, if the import, export or generation operation is set to Never, any user will not be allowed to perform the operation***]

(h) [***In phase 7, if the export operation is set to Always, any user will be allowed to perform the operation***]

Application note:
In phase 6, the entity with the role "Personalisation Agent" always has the security attribute "Key export Management, "Key import Management", and "Key generation Management" set to "authorized".
In phase 7, depending on the use case, the "role" allowed to import, generate or export the keys may be restricted to "Signatory", "User_Admin", "SCA", CGA", "IFD" or "SSCD type 1", or any combination of them.

FDP ACF.1.3/ Key Management SFP
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***none***]

FDP_ACF.1.4/ Key Management SFP
The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [***none***]

6.1.2.3.5 FDP_ETC : Export to outside TSF control

6.1.2.3.5.1 Keys Transfer

FDP_ETC.1.1/ Keys transfer
The TSF shall enforce the [***Key Management SFP***] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2/ Keys transfer
The TSF shall export the user data without the user data's associated security attributes.

6.1.2.3.6 FDP_ITC Import from outside TSF control

6.1.2.3.6.1 Keys import

FDP_ITC.1.1/ Keys
The TSF shall enforce the [***Key Management SFP***] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/ Keys

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/ Keys
The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [***Keys shall be sent by the User with the "role" set to "Signatory", "User_Admin", "Personalisation Agent", "SCA", "CGA", "IFD" or "SSCD type 1"***].

Application note:
In phase 7, depending on the use case, the "role" allowed to import, generate or export the keys may be restricted to "Signatory", "User_Admin", "SCA", CGA", "IFD" or "SSCD type 1", or any combination of them.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

6.1.2.3.7 FIA_AFL Authentication failure

FIA_AFL apply to the authentication mechanisms based on cryptographic keys. The following authentication mechanisms are concernend:

- Authentication of the role “Personalisation Agent”
- Authentication of the role “TOE_Administrator”
- Authentication of the role “User_Admin”
- Authentication of the role “SCA”, “CGA”, “SSCD type 1” and “IFD”.
- Authentication of the remote IT entities “SCA”, “CGA”, “SSCD type 1” and “IFD”

FIA AFL.1.1/ Authentication keys
The TSF shall detect when [***selection :[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]***] unsuccessful authentication attempts occur related to [***consecutive failed authentication attempts***].

FIA AFL.1.2/ Authentication keys
When the defined number of unsuccessful authentication attempts has been [***met or surpassed***], the TSF shall [***assignment : list of actions***].

Refinements:

Type of entity	*Entity*	*Selection for FIA_AFL.1.1*	*list of actions*
User	“Personalisation Agent”	***Positive integer number ‘1’***	***Time of next authentication increases***
User	“TOE_Administrator”	***Positive integer number ‘1’***	***Time of next authentication increases***
User	“User_Admin” (when using symmetric role authentication)	***Administrator configurable positive integer ‘N’*** ***0 ≤N ≤15***	***If N= ‘0’, no actions are taken.*** ***If N != ‘0’, the key is blocked***
User	“SCA”, “CGA”, “SSCD type 1” and “IFD” (when using symmetric device authentication)	***Administrator configurable positive integer ‘N’*** ***0 ≤N ≤15***	***If N= ‘0’, no actions are taken.*** ***If N != ‘0’, the key is blocked***
User	“User_Admin” (when using asymmetric role authentication)	***Positive integer number ‘1’***	***The key is deallocated with respect to FDP_RIP.1.1***

User	"SCA", "CGA", "SSCD type 1" and "IFD" (when using asymmetric device authentication)	***Positive integer number '1'***	***The key is deallocated with respect to FDP_RIP.1.1***
Remote IT entity	"SCA", "CGA", "SSCD type 1" and "IFD" (when using symmetric device authentication)	***Administrator configurable positive integer 'N'*** ***0 ≤N ≤15***	***If N= '0', no actions are taken.*** ***If N != '0', the key is blocked***
Remote IT entity	"SCA", "CGA", "SSCD type 1" and "IFD" (when using asymmetric device authentication)	***Positive integer number '1'***	***The key is deallocated with respect to FDP_RIP.1.1***

6.1.2.3.8 FIA_ATD User attribute definition

FIA ATD.1.1 / S.Admin, S.TOE_Admin, S.Personalizer
The TSF shall maintain the following list of security attributes belonging to individual users [***Authentication key***]

Application Note:
Each role is authenticated using an authentication protocol with a dedicated authentication key. The key to use is a TSF data that is either permanently stored in the TOE, or an ephemeral key extracted from a certificate.

6.1.2.3.9 FMT_MSA Management of security attributes

FMT_MSA.1.1/ Key Management
The TSF shall enforce the [***Key Management SFP***] to restrict the ability to [***modify***] the security attributes [***Key import management, Key generation management and Key export Management***] to [***"Signatory", "User_Admin", "personalisation Agent", "SCA", "CGA", "SSCD type 1", "IFD"***].

FMT_MSA.1.1/ Management of TOE
The TSF shall enforce the [***IAS ECC Administration SFP***] to restrict the ability to [***modify***] the security attributes [***Medium, HashOffCard, SymAuthMechanism and AsymAuthMechanism***] to [***"TOE_Administrator" or "personalisation Agent"***].

6.1.2.3.10 FMT_MTD Management of TSF data

6.1.2.3.10.1 Administrator

FMT_MTD.1.1/ Admin
The TSF shall restrict the ability to [***create***] the [***container of RAD, SCD, SVD and keys***] to [***Administrator***].

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

6.1.2.3.11 FMT_SMF Specification of Management Functions

FMT_SMF.1.1
The TSF shall be capable of performing the following management functions: [
(a) ***SCD/SVD Generation***
(b) ***SCD import***
(c) ***RAD personalisation***
(d) ***RAD unblocking***
(e) ***Signature creation***
(f) ***Management of the TOE***
(g) ***Key Management***].

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

6.2 Security Assurance Requirements

This chapter defines the list of the assurance measures required for the TOE security assurance requirements. The EAL5+ is claimed.

6.2.1 Evaluation Assurance Level rationale

The following assurance packages are required:

Measures	Name
ADV	Development
AGD	Guidance
ALC	Life Cycle
ASE	Security target
ATE	Tests
AVA	Vulnerability

6.2.1.1 ADV : Development

The following components are included:

Measures	Level
ADV_ARC	1
ADV_FSP	5
ADV_IMP	1
ADV_INT	2
ADV_SPM	N/A

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

ADV_TDS	4

6.2.1.2 AGD : Guidance

The following components are included:

Measures	Level
AGD_OPE	1
AGD_PRE	1

6.2.1.3 ALC : Life cycle

The following components are included:

Measures	Level
ALC_CMC	4
ALC_CMS	5
ALC_DEL	1
ALC_DVS	2 - augmented
ALC_FLR	N/A
ALC_LCD	1
ALC_TAT	2

6.2.1.4 ASE : Security target

The following components are included:

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

Measures	Level
ASE_CCL	1
ASE_ECD	1
ASE_INT	1
ASE_OBJ	2
ASE_REQ	2
ASE_SPD	1
ASE_TSS	1

6.2.1.5 ATE : Tests

The following components are included:

Measures	Level
ATE_COV	2
ATE_DPT	3
ATE_FUN	1
ATE_IND	2

6.2.1.6 AVA : Vulnerability

The following components are included:

Measures	Level
AVA_VAN	5 - augmented

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

6.2.2 Rationale for augmentation

6.2.2.1 AVA_VAN.5 Advanced methodical vulnerability analysis

Due to the definition of the TOE, it must be shown to be highly resistant to penetration attacks. This assurance requirement is achieved by the AVA_VAN.5 component. Independent vulnerability analysis is based on highly detailed technical information. The attacker is assumed to be thoroughly familiar with the specific implementation of the TOE. The attacker is presumed to have a high level of technical sophistication.

All the dependencies of AVA_VAN.5, listed below are fulfilled:

- ADV_ARC.1
- ADV_FSP.4
- ADV_TDS.3
- ADV_IMP.1
- AGD_OPE.1
- AGD_PRE.1
- ATE_DPT.1

6.2.2.2 ALC_DVS.2 Sufficiency of security measures

In order to protect the TOE on development Phase, the component ALC_DVS.2 was added. This latter requires security documentation justifying that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

ALC_DVS.2 does not have any dependencies.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

6.3 Security Requirements Rationale

6.3.1 Security Objectives of the TOE rationale

6.3.1.1 Rationale

In the following chapter, all refinements to of the [SSCD2] and [SSCD3] are indicated in *blue italic letters*.

OT.EMSEC_Design (Provide physical emanations security)

covers that no intelligible information is emanated. This is provided by **FPT_EMSEC.1**

OT.Lifecycle_Security (Lifecycle security)

is provided by the security assurance requirements ALC_DVS.2, ALC_LCD.1, ALC_TAT.1, ALC_DEL.2, and ALC_DEL.1 that ensure the lifecycle security during the development, configuration and delivery phases of the TOE. The test functions **FPT_TST.1** [and FPT_TEE.1] provide failure detection throughout the lifecycle. **FCS_CKM.4.1/SCD/SVD** provides secure destruction of the SCD to conclude the operational usage of the TOE as SSCD.

OT.SCD_Secrecy (Secrecy of signature-creation data)

counters that, with reference to recital (18) of the Directive, storage or copying of SCD causes a threat to the legal validity of electronic signatures. OT.SCD_Secrecy is provided by the security functions specified by ***FMT_SMF.1,*** **FDP_ACC.1/Initialisation SFP** and **FDP_ACF.1/ Initialisation SFP** that ensure that only authorised user can initialise the TOE and create or load the SCD. The authentication and access management functions specified by **FMT_MOF.1**, **FMT_MSA.1/Administrator - Import** and **FMT_MSA.1/Administrator - Initialisation**, ***FMT_MSA.2***, **FMT_MSA.3**, and **FMT_SMR.1** ensure that only the signatory can use the SCD and thus avoid that an attacker may gain information on it.

The security functions specified by **FDP_RIP.1** and **FCS_CKM.4.1/SCD/SVD** ensure that residual information on SCD is destroyed after the SCD has been used for signature creation and that destruction of SCD leaves no residual information. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD.

The security functions specified by **FDP_SDI.2/Persistent** ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. [FPT_TEE.1 and] **FPT_FLS.1** tests the working conditions of the TOE and guarantee a secure state when integrity

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

is violated and thus assure that the specified security functions are operational. An example where compromising error conditions are countered by **FPT_FLS** is differential fault analysis (DFA).

The assurance requirements ADV_IMP.1 by requesting evaluation of the TOE implementation, and AVA_VAN.5 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient.

OT.SCD_SVD_Corresp (Correspondence between SVD and SCD)

addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by **FCS_CKM.1.1** to generate corresponding SVD/SCD pairs (if it is generated).The security functions specified by **FDP_SDI.2/Persistent** ensure that the keys are not modified, so to retain the correspondence. Cryptographic correspondence is provided by **FCS_COP.1/CORRESP**.

OT.SVD_Auth_TOE (TOE ensures authenticity of the SVD)

is provided by a trusted channel guaranteeing SVD origin and integrity by means of **FTP_ITC.1/SVD Transfer** and **FDP_UIT.1/SVD Transfer**. The cryptographic algorithms specified by **FDP_ACC.1/SVD Transfer SFP**, **FDP_ACF.1/SVD Transfer SFP** and **FDP_ETC.1/SVD Transfer** and **FMT_SMR.1** *with* ***FMT_SMF.1*** ensure that only authorised user can Import the SVD from a SSCD Type1 and Export the SVD to the CGA.

The security functions specified by ***FDP_SDI.2/Persistent*** *ensure the SVD(s) stored in the TOE is(are) authentic.*

In Phase 7, the mutual authentication between the TOE and the CGA that takes place thanks to ***FCS_RNG.1*** *and* ***FCS_COP.1.1/ Symmetric Device Authentication*** *or* ***FCS_RNG.1, FCS_COP.1.1/Diffie Hellmann Computation***, ***FCS_COP.1.1/Certificate verification***, ***FCS_COP.1.1/Asymmetric Internal DAPP Authentication***, ***FCS_COP.1.1/Asymmetric External DAPP Authentication*** *enable to establish a trusted channel as mandated by* ***FTP_ITC.1/SVD Transfer.*** *During the mutual authentication, SM session keys are generated with* ***FCS_CKM.1.1/Session keys*** *and* ***FCS_COP.1.1/Data hashing*** *from random number generated by the TOE (with* ***FCS_RNG.1****) and the CGA. These session keys are used for a MAC computation with* ***FCS_COP.1.1/Secure Messaging in Integrity*** *to ensure the fulfilment of* ***FDP_UIT.1/SVD Transfer.*** *Moreover as the MAC is computed using a counter (SSC), incremented at each new exchange, any deletion or replay of command is deleted as requested by* ***FDP_UIT.1/SVD Transfer.***

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

*In phase 6, the SVD may be transferred by the TOE to the Personalisation Agent that is mingled with the CGA. A mutual authentication between both entities takes place using the GP authentication protocol as mandated by **FCS_COP.1.1/GP Authentication.** During this authentication, a session encryption key is agreed between the TOE and the Personalisation Agent/CGA. This key is then used by the TOE to sign the footprint of the SVD computed using **FCS_COP.1.1/Data hashing** and **FCS_COP.1.1/GP secret data Protection.** This signature ensures the fulfilment of **FDP_UIT.1/SVD Transfer**, as well as **FTP_ITC.1/SVD Transfer.***

OT.Tamper_ID (Tamper detection)

is provided by **FPT_PHP.1** by the means of passive detection of physical attacks.

OT.Tamper_Resistance (Tamper resistance)

is provided by **FPT_PHP.3** to resist physical attacks.

OT.Init (SCD/SVD generation)

addresses that generation of a SCD/SVD pair requires proper user authentication. ***FIA_ATD.1.1/S.Signatory*** *(for the signatory) and* ***FIA_ATD.1.1/S.Admin*** *(for the administrator if it uses also a RAD)* define RAD as user attribute *and* ***FIA_ATD.1.1/S.Admin, S.TOE_Admin, S.Personalizer*** defines the *authentication keys* as the corresponding administrator attribute (if it uses an authentication mechanism using a key). The TSF specified by **FIA_UID.1** and **FIA_UAU.1** provide user identification and user authentication prior to enabling access to authorised functions. The attributes of the authenticated user are provided by **FMT_MSA.1/Administrator - Initialisation**, ***FMT_MSA.2,*** **FMT_MSA.3** for static attribute initialisation. Access control is provided by **FDP_ACC.1/Initialisation SFP** and **FDP_ACF.1/ Initialisation SFP,** ***FMT_SMF.1,*** *and* ***FMT_SMR.1***. Effort to bypass the access control by a frontal exhaustive attack is blocked by **FIA_AFL.1/RAD** *(for authentication based on RAD) and* ***FIA_AFL.1/Authentication keys*** *(for authentication using cryptographic keys)*.

OT.SCD_Unique (Uniqueness of the signature-creation data)

implements the requirement of practically unique SCD as laid down in the Directive [1], Annex III, article 1(a), which is provided by the cryptographic algorithms specified by **FCS_CKM.1.1**.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

OT.SCD_Transfer (Secure transfer of SCD between SSCD)

is provided by **FDP_ITC.1/SCD** and **FDP_UCT.1/Receiver** that ensure that a trusted channel is provided and that confidentiality is maintained. Security functions specified by **FDP_ACC.1/SCD Import SFP**, ***FMT_MSA.1.1 / Administrator – Import*** **,** **FMT_MSA.2**, **FMT_MSA.3**, **FMT_SMR.1**, ***FMT_SMF.1*** and **FDP_ACF.1/SCD Import SFP** ensure that transfer of SCDs is restricted to administrators. This supports the confidentiality-oriented functions. Security function **FCS_CKM.4.1/SCD/SVD** destroys the SCD before a SCD is re-imported into the TOE.

In Phase 7, the mutual authentication between the TOE and the SCA that takes place thanks to ***FCS_RNG.1*** *and* ***FCS_COP.1.1/ Symmetric Device Authentication*** *or* ***FCS_RNG.1, FCS_COP.1.1/Diffie Hellmann Computation***, ***FCS_COP.1.1/Certificate verification***, ***FCS_COP.1.1/Asymmetric Internal DAPP Authentication***, ***FCS_COP.1.1/Asymmetric External DAPP Authentication*** *enable to establish a trusted channel as mandated by* ***FTP_ITC.1/SCD Import.*** *During the mutual authentication, SM session keys are generated with* ***FCS_CKM.1.1/Session keys*** *and* ***FCS_COP.1.1/Data hashing*** *from random number generated by the TOE (with* ***FCS_RNG.1****) and the SSCD type 1. These session keys are used to encrypt the SCD with* ***FCS_COP.1.1/Secure Messaging in Confidentiality*** *to ensure the fulfilment of* ***FDP_UCT.1/Receiver.*** *Moreover, as* ***FDP_UCT.1/Receiver*** *always go with integrity and authenticity supported by* ***FCS_COP.1.1/Secure Messaging in Integrity****, the SCD import procedure also ensures integrity and authenticity of the SCD.*

In phase 6, the SCD may be received from the Personalisation Agent that is mingled with the SSCD type 1. A mutual authentication between both entities takes place using the GP authentication protocol as mandated by ***FCS_COP.1.1/GP Authentication.*** *During this authentication, a session encryption key is agreed between the TOE and the Personalisation Agent/SSCD type 1, and used by the TOE to decrypt the SCD using* ***FCS_COP.1.1/GP secret data Protection,*** *which ensures the fulfilment of* ***FTP_ITC.1/SCD Import****. Moreover, as the session encryption key used to send the SCD to the TOE is unknown to attacker, any attempt to modify the SCD during its import, would cause the decrypted SCD to be inconsistent. This inconsistency will be detected by TOE using* ***FPT_TST.1*** *and* ***FCS_COP.1.1/CORRESP****. This ensures that the communication channel between the TOE and the Personalisation Agent/SSCD type 1 is a trusted channel in the sense of* ***FTP_ITC/SCD import.***

OT.DTBS_Integrity_TOE (Verification of DTBS-representation integrity)

covers that integrity of the DTBS-representation to be signed is to be verified, as well as the DTBS-representation is not altered by the TOE. This is provided by the trusted channel integrity verification mechanisms of **FDP_ITC.1/DTBS**, **FTP_ITC.1/DTBS Import**, and by **FDP_UIT.1/TOE DTBS**. The verification that the DTBS-representation has not been altered by the TOE is done by integrity

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

functions specified by **FDP_SDI.2/DTBS**. The access control requirements of **FDP_ACC.1/Signature-creation SFP** and **FDP_ACF.1/Signature-creation SFP** keeps unauthorised parties off from altering the DTBS-representation.

*The DTBS is sent to the TOE during the signature creation covered by **FMT_SMF.1**. The mutual authentication between the TOE and the SCA that takes place thanks to **FCS_RNG.1** and **FCS_COP.1.1/ Symmetric Device Authentication** or **FCS_RNG.1, FCS_COP.1.1/Diffie Hellmann Computation, FCS_COP.1.1/Certificate verification, FCS_COP.1.1/Asymmetric Internal DAPP Authentication, FCS_COP.1.1/Asymmetric External DAPP Authentication** enable to establish a trusted channel as mandated by **FTP_ITC.1/DTBS Import.** During the mutual authentication, SM session keys are generated with **FCS_CKM.1.1/Session keys** and **FCS_COP.1.1/Data hashing** from random number generated by the TOE (with **FCS_RNG.1**) and the SCA. These session keys are used for a MAC computation with **FCS_COP.1.1/Secure Messaging in Integrity** to ensure the fulfilment of **FDP_UIT.1/TOE DTBS.** Moreover as the MAC is computed using a counter (SSC), incremented at each new exchange, any deletion or replay of command is deleted as requested by **FDP_UIT.1/TOE DTBS.***

OT.Sigy_SigF (Signature generation function for the legitimate signatory only)

is provided by **FIA_UAU.1** and **FIA_UID.1** that ensure that no signature generation function as defined in **FMT_SMF.1** can be invoked before the signatory is identified and authenticated. The security functions specified by **FDP_ACC.1/Personalisation SFP**, **FDP_ACC.1/Signature-creation SFP**, **FDP_ACF.1/Personalisation SFP**, **FDP_ACF.1/Signature-creation SFP**, **FMT_MTD.1.1/Signatory**, **FMT_MTD.1.1/Admin** and **FMT_SMR.1** ensure that the signature process is restricted to the signatory.

The security functions specified by **FIA_ATD.1.1/S.Signatory**, **FMT_MOF.1**, **FMT_MSA.2**, **FMT_MSA.3** ensure that the access to the signature generation functions remain under the sole control of the signatory, as well as **FMT_MSA.1/Signatory** provides that the control of corresponding security attributes is under signatory's control. The security functions specified by **FDP_SDI.2/Persistent** and **FTP_TRP.1/TOE** ensure the integrity of stored data both during communication and while stored.

The security functions specified by **FDP_RIP.1** and **FIA_AFL.1/RAD** provide protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication.

The assurance measures specified by AVA_VAN.5 by requesting that the TOE resists attacks with a high attack potential assures that the security functions are efficient.

***FMT_MTD.1/Unblock** ensures the unblocking of the RAD is made under the sole control of the administrator.*

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

*In phase 6, the RAD (PIN or Biometric Data) may be loaded on the TOE by the Personalisation Agent as defined in **FMT_SMF.1** according to the access control laid down in **FDP_ACC.1/Personalisation** and **FDP_ACF.1/Personalisation**. The Personalisation Agent is authenticated with a mutual authentication performed with **FCS_RNG.1** and **FCS_COP.1/GP Authentication,** and is authenticated with **FMT_SMR.1. FIA_ATD.1.1/S.Admin, S.TOE_Admin, S.Personalizer** defines the authentication keys as the corresponding Personalization Agent attribute. Effort to bypass the access control by a frontal exhaustive attack is blocked by **FIA_AFL.1/Authentication keys**. During the mutual authentication, a session encryption key is agreed between the TOE and the Personalisation Agent and used by the TOE to decrypt the RAD using **FCS_COP.1.1/GP secret data Protection**, ensuring the confidentiality of the RAD during its transfer in phase 6.*

*In phase 6, **FMT_MSA.1.1/ Signatory** guarantees that the Personalisation Agent can not sign on behalf on the signatory, ensuring the signature creation features remains under the sole control of the signatory.*

OT.Sig_Secure (Cryptographic security of the electronic signature)

is provided by the cryptographic algorithms specified by **FCS_COP.1/SIGNING** and **FCS_COP.1.1/Data hashing** which ensure the cryptographic robustness of the signature algorithms. The security functions specified by [FPT_TEE.1 and] **FPT_TST.1** ensure that the security functions are performing correctly. **FDP_SDI.2/Persistent** corresponds to the integrity of the SCD implemented by the TOE.

*The way the electronic signature is computed may be controlled by the "TOE_Administrator" that may enforce the TOE to compute electronic signatures only over DTBS representation computed by the TOE (data hashing done by the TOE). The management of this function is protected by the proper "TOE_Administrator" authentication with **FIA_ATD.1.1/S.Admin, S.TOE_Admin, S.Personalizer** which defines the authentication keys as the corresponding "TOE_Administrator" attribute. The TSF specified by **FIA_UID.1** and **FIA_UAU.1** provide "TOE_Administrator" identification and authentication prior to enabling access to authorised functions. The attributes of the authenticated "TOE_Administrator" are provided by **FMT_MSA.1/Management of TOE**, **FMT_MSA.2** and **FMT_MSA.3** for static attribute initialisation. Access control is provided by **FDP_ACC.1/IAS ECC Administration SFP, FDP_ACF.1/ IAS ECC Administration SFP, FMT_SMR.1** and **FMT_SMF.1**. Effort to bypass the access control by a frontal exhaustive attack is blocked by **FIA_AFL.1/Authentication keys**.*

OT.Authentication_Secure (Secure authentication mechanisms)

is provided by the cryptographic algorithms specified by (1) **FCS_COP.1.1/Diffie Hellman**, **FCS_COP.1.1/Certificate verification** , **FCS_COP.1.1/Asymmetric Internal DAPP Authentication**, **FCS_COP.1.1/Asymmetric External DAPP Authentication** and **FCS_RNG.1** for the mutual

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

authentication based on an asymmetric scheme (DAPP), (2) **FCS_RNG.1** and **FCS_COP.1.1/Symmetric Device authentication** for the mutual authentication based on symmetric scheme, (3) **FCS_RNG.1** and **FCS_COP.1.1/GP Authentication** for the authentication of the personalisation agent and of the "TOE_Administrator", (4) **FCS_RNG.1** and **FCS_COP.1.1/Symmetric Role Authentication** for the authentication of an entity based on a symmetric scheme, (5) **FCS_COP.1.1/Certificate verification** , **FCS_COP.1.1/Asymmetric Role Authentication**, and **FCS_RNG.1** for the authentication of an entity based on an asymmetric scheme. All these requirements ensure the cryptographic robustness of the authentication mechanisms.

The use of a challenge freshly generated by the TOE with **FCS_RNG.1** in theses authentication protocols ensures a protection against replay attacks when authenticating remote entities. **FIA_AFL.1/Authentication keys** ensures a correct detection and protection of authentication failure or exhaustive attacks. The security function specified by **FPT_TST.1** ensures that the security functions are performed correctly and **FDP_SDI.2/Persistent** guarantees the integrity of the authentication key(s) used by the TOE. **FMT_SMR.1** and **FMT_SMF.1** ensure the TOE can distinguish between external entities successfully authenticated ("IFD", "SCA", "CGA", "SSCD type 1", "User_Admin", "Personalisation Agent", "TOE_Administrator"), including different users "User_Admin" and can grant them dedicated rights.

In case of authentication protocols involving the import of ephemeral public key (EPHEMERAL_KEYS) on the TOE (using Card verifiable certificates), **FDP_RIP.1** ensures that the key value is not kept by the TOE after usage and then can not be reused for a replay attack.

This objective ensures as well the establishment of a trusted channel following a successful mutual authentication ((1) and (2)). This trusted channel ensures authenticity, integrity and confidentiality of communication. **FCS_CKM.1.1 /Session keys** and **FCS_COP.1.1/Data hashing** generates session keys for the secure communication from a common secret agreed between the TOE and the external entity during the mutual authentication procedure.

Any incoming command shall contain a MAC computed by the issuer with the session key agreed during the mutual authentication, so that any unauthenticated or non integer command is detected by the MAC verification performed by the TOE using **FCS_COP.1.1/Secure messaging in integrity.** The data exchanged through this trusted channel are also protected in confidentiality thanks to **FCS_COP.1.1/Secure messaging in confidentiality**, ensuring they can only be disclosed to the parties authenticated during the mutual authentication step. The encryption key is ephemeral as it is generated during the mutual authentication using a challenge freshly generated by the TOE using **FCS_RNG.1**, which ensures that dictionary attacks can not be performed on encrypted data. When an integrity error is detected, or if the MAC is wrong (wrong authentication of the command issuer), the session keys (for integrity and confidentiality) are erased thanks to **FCS_CKM.4.1/Session keys** so that they can not be reused anymore, causing the trusted channel to be irreversibly lost. In particular, it ensures that encrypted data that may be caught by an attacker can not be reused anymore to masquerade the TOE.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

The type of authentication scheme used by the TOE to authenticate the administrator or perform a mutual authentication may be controlled by the "TOE_Administrator". It may enforce the TOE to allow the use of symmetric scheme ((2) and (4)) and/or asymmetric ((1) and (5)) schemes. The management of this function is protected by the proper "TOE_Administrator" authentication using **FIA_ATD.1.1/S.Admin, S.TOE_Admin, S.Personalizer** which defines the authentication keys as the corresponding "TOE_Administrator" attribute. The TSF specified by **FIA_UID.1** and **FIA_UAU.1** provide "TOE_Administrator" identification and authentication prior to enabling access to authorised functions. The attributes of the authenticated "TOE_Administrator" are provided by **FMT_MSA.1/Management of TOE**, **FMT_MSA.2**, and **FMT_MSA.3** for static attribute initialisation. Access control is provided by **FDP_ACC.1/IAS ECC Administration SFP, FDP_ACF.1/ IAS ECC Administration SFP**, **FMT_SMR.1** and **FMT_SMF.1**. Effort to bypass the access control by a frontal exhaustive attack is blocked by **FIA_AFL.1/Authentication keys**.

This objective ensures as well that any authentication key is loaded in the TOE by an authenticated user, so that only genuine keys associated to genuine users are declared to the TOE. The key import defined by **FMT_SMF.1** is protected by access control as mandated by **FDP_ACF.1/ Key Management SFP** and **FDP_ACC.1/ Key Management SFP.** It is protected by the proper Agent(s) authentication that cannot be bypassed to access these functions with the TSF specified by **FIA_UID.1** and **FIA_UAU.1.** The agent entitled to load the authentication key is (are) authenticated with **FMT_SMR.1. FIA_ATD.1.1/S.Signatory**, **FIA_ATD.1.1/S.Admin**, define the **RAD** as corresponding Agent attribute (for Administrator and Signatory) and **FIA_ATD.1.1/S.Admin, S.TOE_Admin, S.Personalizer** defines the authentication keys as the corresponding Agent attribute (for Administrator and Personalization Agent) and ensure that the sole Agent can realize these functions. Effort to bypass the access control by a frontal exhaustive attack is blocked by **FIA_AFL.1/RAD** and **FIA_AFL.1/Authentication keys**.

OT.SCD/SVD_Management (Management of SCD/SVD)

The link between the SCD and the matching certificate is ensured by **FMT_MTD.1.1/Association between SCD and SCD_ID** that guarantees and unambiguous link between the SCD and its identifier, which is connected to the certificate.

OT.Key_LifeCycle_Security (Lifecycle security of the key(s) stored in the TOE)

is provided by the security assurance requirements ALC_DVS.2, ALC_LCD.1, ALC_TAT.2, and ALC_DEL.1 that ensure the lifecycle security during the development, configuration and delivery phases of the TOE. The test functions **FPT_TST.1** provides failure detection throughout the lifecycle.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FCS_CKM.4.1/SCD/SVD provides secure destruction of the key(s) in case of generation or import of authentication or eServices keys.

OT.Key_Secrecy (Secrecy of key(s) stored in the TOE)

is provided by the security functions specified by **FMT_SMF.1**, **FDP_ACC.1/ Key Management SFP** and **FDP_ACF.1/ Key Management SFP** that ensure that only authorised user can generate or import keys into the TOE. The authentication and access management functions specified by **FMT_MSA.1/Key Management**, **FMT_MSA.2, FMT_MSA.3**, **FMT_SMR.1** ensure that only the authenticated entity can use the key(s) and thus avoid that an attacker may gain information on it.

The security requirement **FDP_ITC.1/Keys** controls the keys import and **FDP_ETC.1/Keys transfer** controls the key export.

The security functions specified by **FDP_RIP.1** and **FCS_CKM.4.1/SCD/SVD** ensure that residual information on a key(s) is destroyed after a key has been used for authentication (verification or proof) or an eServices keys has been used and that destruction of key(s) leaves no residual information.

Cryptographic quality of the asymmetric key pair(s) shall prevent disclosure of the TOE's private authentication key(s) and eServices key(s) by cryptographic attacks using the publicly known public key.

The security functions specified by **FDP_SDI.2/Persistent** ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the authentication key. **FPT_FLS.1** tests the working conditions of the TOE and guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS is differential fault analysis (DFA).

The assurance requirements ADV_IMP.1 by requesting evaluation of the TOE implementation, and AVA_VAN.5 by requesting that the TOE resists attacks with a high attack potential assure that the security functions are efficient.

OT.TOE_AuthKey_Unique (Uniqueness of the TOE authentication key(s))

implements the requirement of practically unique TOE's authentication private key, which is provided by the cryptographic algorithms specified by **FCS_CKM.1.1**.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

OT.LifeCycle_Management (Management of the TOE life cycle)

ensures a correct separation of the TOE life cycle between phase 6 and 7.

In phase 6, **FMT_MTD.1.1/TOE State** ensures the TOE irreversibly switches from phase 6 to phase 7 under the sole control of the Personalization Agent. The Personalisation Agent is authenticated with a mutual authentication performed with **FCS_RNG.1** and **FCS_COP.1/GP Authentication** and is authenticated with **FMT_SMR.1. FIA_ATD.1.1/S.Admin, S.TOE_Admin, S.Personalizer** defines the authentication keys as the corresponding Personalization Agent attribute. Effort to bypass the access control by a frontal exhaustive attack is blocked by **FIA_AFL.1/Authentication keys**.

In phase 7, **FDP_ACC.1/Signature creation SFP , FDP_ACC.1/SVD transfer SFP , FDP_ACC.1/Initialisation SFP , FDP_ACC.1/Personalisation SFP , FDP_ACC.1/SCD import SFP , FDP_ACC.1/IAS ECC Administration SFP , FDP_ACC.1/Key Management SFP , FDP_ACF.1/Signature creation SFP , FDP_ACF.1/SVD transfer SFP , FDP_ACF.1/Initialisation SFP , FDP_ACF.1/Personalisation SFP , FDP_ACF.1/SCD import SFP , FDP_ACF.1/IAS ECC Administration SFP, FDP_ACF.1/Key Management SFP, FMT_MTD.1/Unblock, FMT_MOF.1, FMT_MTD.1/Admin, FMT_MTD.1/Signatory** ensures the Personalization Agent does not control the TOE anymore.

In phase 6, the Personalization Agent has complete control over the administrative functions of the TOE. It is authenticated with a mutual authentication performed with **FCS_RNG.1** and **FCS_COP.1/GP Authentication** and is authenticated with **FMT_SMR.1**. It may import, erase, generate SCD/SVD, export SVD, manage Keys, create RAD and manage the configuration of the TOE as mandated in **FMT_SMF.1**, according to the security policies defined in **FDP_ACC.1/SVD transfer SFP , FDP_ACC.1/Initialisation SFP , FDP_ACC.1/Personalisation SFP , FDP_ACC.1/SCD import SFP , FDP_ACC.1/IAS ECC Administration SFP , FDP_ACC.1/Key Management SFP , FDP_ACF.1/SVD transfer SFP , FDP_ACF.1/Initialisation SFP , FDP_ACF.1/Personalisation SFP , FDP_ACF.1/SCD import SFP , FDP_ACF.1/IAS ECC Administration SFP, FDP_ACF.1/Key Management SFP, FDP_ETC.1/SVD Transfer, FDP_ETC.1/Keys transfer.** It may as well change TOE State (**FMT_MTD.1.1/TOE State**), load the serial number of the TOE (**FMT_MTD.1.1/TOE Serial Number).** These functions are protected by the Personalisation Agent authentication that cannot be bypassed to access these functions with the TSF specified by **FIA_UID.1** and **FIA_UAU.1**. **FIA_ATD.1.1/S.Admin, S.TOE_Admin, S.Personalizer** defines the authentication keys as the corresponding Personalization Agent attribute and **FMT_MSA.1/Administrator – Initialisation, FMT_MSA.1/Administrator – Import, FMT_MSA.1/Management of TOE, FMT_MSA.1/Key Management**, **FMT_MSA.2**, **FMT_MSA.3** that ensure that the sole Personalisation Agent can realize these functions. Effort to bypass the access control by a frontal exhaustive attack is blocked by **FIA_AFL.1/Authentication keys**.

OT.eServices (Provision of eServices)

is provided by the cryptographic mechanisms specified by (1) **FCS_COP.1.1/Diffie Hellman**, (2) **FCS_COP.1.1/Certificate verification**, (3) **FCS_COP.1.1/C/S Authentication**, (4) **FCS_COP.1.1/Encryption key decipherment**. These requirements ensure the cryptographic robustness of these eServices.

The eServices keys may be loaded, generated, and the matching public key may be exported as required by **FMT_SMF.1**. The Agent(s) entitled to perform such operations shall be authenticated with **FMT_SMR.1** using cryptographic protocols (1) **FCS_COP.1.1/Diffie Hellman**, **FCS_COP.1.1/Certificate verification** , **FCS_COP.1.1/Asymmetric Internal DAPP Authentication**, **FCS_COP.1.1/Asymmetric External DAPP Authentication** and **FCS_RNG.1** for the mutual authentication based on an asymmetric scheme (DAPP), (2) **FCS_RNG.1** and **FCS_COP.1.1/Symmetric Device authentication** for the mutual authentication based on symmetric scheme, (3) **FCS_RNG.1** and **FCS_COP.1.1/Symmetric Role Authentication** for the authentication of an entity based on a symmetric scheme, (4) **FCS_COP.1.1/Certificate verification** , **FCS_COP.1.1/Asymmetric Role Authentication**, and **FCS_RNG.1** for the authentication of an entity based on an asymmetric scheme. These functions are protected by the proper Agent(s) authentication that cannot be bypassed to access these functions with the TSF specified by **FIA_UID.1** and **FIA_UAU.1**. **FIA_ATD.1.1/S.Signatory**, **FIA_ATD.1.1/S.Admin**, define the **RAD** as corresponding Agent attribute (for Administrator and Signatory) and **FIA_ATD.1.1/S.Admin, S.TOE_Admin, S.Personalizer** defines the authentication keys as the corresponding Agent attribute (for Administrator and Personalisation Agent) and ensure that the sole Agent can realize these functions. Effort to bypass the access control by a frontal exhaustive attack is blocked by **FIA_AFL.1/RAD** and **FIA_AFL.1/Authentication keys**.

6.3.2 Security functional requirements analysis

6.3.2.1 Dependencies analysis

The following table lists for each SFRs its dependencies, and highlights the non satisfied dependencies.

SFRs	Dependencies	Satisfied dependencies
FCS_CKM.1.1	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1.1 / CORRESP FCS_COP.1.1 / SIGNING FCS_COP.1.1 / C/S Authentication FCS_COP.1.1 / Encryption key decipherment FCS_COP.1.1 / Certificate verification FCS_COP.1.1 / Asymmetric Internal DAPP Authentication FCS_CKM.4.1 / SCD/SVD

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

		(FMT_MSA.2.1)
FCS_CKM.1.1 / Session keys	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1.1 / Secure Messaging in Integrity FCS_COP.1.1 / Secure Messaging in Confidentiality FCS_CKM.4.1 / Session keys
FCS_CKM.4.1 / SCD/SVD	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FDP_ITC.1.1 / SCD FDP_ITC.1.2 / SCD FDP_ITC.1.3 / SCD FDP_ITC.1.1 / Keys FDP_ITC.1.2 / Keys FDP_ITC.1.3 / Keys FCS_CKM.1.1 (FMT_MSA.2.1)
FCS_CKM.4.1 / Session keys	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FDP_ITC.1.1 / SCD FDP_ITC.1.2 / SCD FDP_ITC.1.3 / SCD FDP_ITC.1.1 / Keys FDP_ITC.1.2 / Keys FDP_ITC.1.3 / Keys FCS_CKM.1.1 /Session keys
FCS_COP.1.1 / CORRESP	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	(FDP_ITC.1.1 / DTBS) (FDP_ITC.1.2 / DTBS) (FDP_ITC.1.3 / DTBS) FCS_CKM.1.1 FCS_CKM.4.1 / SCD/SVD (FMT_MSA.2.1)

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FCS_COP.1.1 / SIGNING	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	(FDP_ITC.1.1 / DTBS) (FDP_ITC.1.2 / DTBS) (FDP_ITC.1.3 / DTBS) FDP_ITC.1.1 / SCD FDP_ITC.1.2 / SCD FDP_ITC.1.3 / SCD FCS_CKM.1.1 FCS_CKM.4.1 / SCD/SVD (FMT_MSA.2.1)
FCS_COP.1.1 / Diffie Hellman computation	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FDP_ITC.1.1 / Keys FDP_ITC.1.2 / Keys FDP_ITC.1.3 / Keys FCS_CKM.4.1 / SCD/SVD
FCS_COP.1.1 / Secure Messaging in confidentiality	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1.1 / Session keys FCS_CKM.4.1 / Session keys
FCS_COP.1.1 / Secure Messaging in integrity	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key	FCS_CKM.1.1 / Session keys FCS_CKM.4.1 / Session keys

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

	destruction	
FCS_COP.1.1 / Data hashing	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	**Non satisfied => See Justification #1**
FCS_COP.1.1 / C/S Authentication	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FDP_ITC.1.1 / Keys FDP_ITC.1.2 / Keys FDP_ITC.1.3 / Keys FCS_CKM.1.1 FCS_CKM.4.1 / SCD/SVD
FCS_COP.1.1 / Encryption key decipherment	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FDP_ITC.1.1 / Keys FDP_ITC.1.2 / Keys FDP_ITC.1.3 / Keys FCS_CKM.1.1 FCS_CKM.4.1 / SCD/SVD
FCS_COP.1.1 / Symmetric Role Authentication	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or	FDP_ITC.1.1 / Keys FDP_ITC.1.2 / Keys FDP_ITC.1.3 / Keys FCS_CKM.1.1 FCS_CKM.4.1 / SCD/SVD

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

	FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	
FCS_COP.1.1 / Symmetric Device Authentication	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FDP_ITC.1.1 / Keys FDP_ITC.1.2 / Keys FDP_ITC.1.3 / Keys FCS_CKM.1.1 FCS_CKM.4.1 / SCD/SVD
FCS_COP.1.1 / Certificate Verification	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	**Non satisfied => See Justification #2**
FCS_COP.1.1 / Asymmetric Role Authentication	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	**Non satisfied => See Justification #3**

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FCS_COP.1.1 / Asymmetric Internal DAPP Authentication	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FDP_ITC.1.1 / Keys FDP_ITC.1.2 / Keys FDP_ITC.1.3 / Keys FCS_CKM.1. FCS_CKM.4.1 / SCD/SVD
FCS_COP.1.1 / Asymmetric External DAPP Authentication	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	**Non satisfied => See Justification #4**
FCS_COP.1.1 / GP Authentication	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	[PLT] FDP_ITC.1.1 / PP Import of user data without security attributes [PLT] FDP_ITC.1.2 / PP Import of user data without security attributes [PLT] FDP_ITC.1.3 / PP Import of user data without security attributes [PLT] FCS_CKM.4.1
FCS_COP.1.1 / GP secret data protection	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key	[PLT] FDP_ITC.1.1 / PP Import of user data without security attributes [PLT] FDP_ITC.1.2 / PP Import of user data without security attributes [PLT] FDP_ITC.1.3 / PP Import of user data without security attributes [PLT] FCS_CKM.4.1

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

	destruction	
FCS_RNG.1.1	N/A	N/A
FCS_RNG.1.2	N/A	N/A
FDP_ACC.1.1 / SVD Transfer SFP	FDP_ACF.1 Security attribute based access control	FDP_ACF.1.1 / SVD Transfer SFP FDP_ACF.1.2 / SVD Transfer SFP FDP_ACF.1.3 / SVD Transfer SFP FDP_ACF.1.4 / SVD Transfer SFP
FDP_ACC.1.1 / Initialisation SFP	FDP_ACF.1 Security attribute based access control	FDP_ACF.1.1 / Initialisation SFP FDP_ACF.1.2 / Initialisation SFP FDP_ACF.1.3 / Initialisation SFP FDP_ACF.1.4 / Initialisation SFP
FDP_ACC.1.1 / Personalization SFP	FDP_ACF.1 Security attribute based access control	FDP_ACF.1.1 / Personalization SFP FDP_ACF.1.2 / Personalization SFP FDP_ACF.1.3 / Personalization SFP FDP_ACF.1.4 / Personalization SFP
FDP_ACC.1.1 / Signature creation SFP	FDP_ACF.1 Security attribute based access control	FDP_ACF.1.1 / Signature creation SFP FDP_ACF.1.2 / Signature creation SFP FDP_ACF.1.3 / Signature creation SFP FDP_ACF.1.4 / Signature creation SFP
FDP_ACC.1.1 / SCD import SFP	FDP_ACF.1 Security attribute based access control	FDP_ACF.1.1 / SCD import SFP FDP_ACF.1.2 / SCD import SFP FDP_ACF.1.3 / SCD import SFP FDP_ACF.1.4 / SCD import SFP
FDP_ACC.1.1 / IAS ECC Administration SFP	FDP_ACF.1 Security attribute based access control	FDP_ACF.1.1 / IAS ECC Administration SFP FDP_ACF.1.2 / IAS ECC Administration SFP FDP_ACF.1.3 / IAS ECC Administration SFP FDP_ACF.1.4 / IAS ECC Administration SFP
FDP_ACC.1.1 / Key Management	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACF.1.1 / Key Management SFP FDP_ACF.1.2 / Key Management SFP FDP_ACF.1.3 / Key Management SFP

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

SFP		FDP_ACF.1.4 / Key Management SFP
FDP_ACF.1.1 / SVD Transfer SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 SVD Transfer SFP FMT_MSA.3.1 FMT_MSA.3.1
FDP_ACF.1.2 / SVD Transfer SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 SVD Transfer SFP FMT_MSA.3.1 FMT_MSA.3.0
FDP_ACF.1.3 / SVD Transfer SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 SVD Transfer SFP FMT_MSA.3.1 FMT_MSA.3.1
FDP_ACF.1.4 / SVD Transfer SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 SVD Transfer SFP FMT_MSA.3.1 FMT_MSA.3.2
FDP_ACF.1.1 / Initialisation SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / Initialisation SFP FMT_MSA.3.1 FMT_MSA.3.1
FDP_ACF.1.2 / Initialisation SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / Initialisation SFP FMT_MSA.3.1 FMT_MSA.3.0
FDP_ACF.1.3 / Initialisation SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / Initialisation SFP FMT_MSA.3.1 FMT_MSA.3.1
FDP_ACF.1.4 / Initialisation SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / Initialisation SFP FMT_MSA.3.1 FMT_MSA.3.2
FDP_ACF.1.1 / Personalization SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / Personalization SFP FMT_MSA.3.1 FMT_MSA.3.1
FDP_ACF.1.2 / Personalization SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / Personalization SFP FMT_MSA.3.1 FMT_MSA.3.0

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FDP_ACF.1.3 / Personalization SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / Personalization SFP FMT_MSA.3.1 FMT_MSA.3.1
FDP_ACF.1.4 / Personalization SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / Personalization SFP FMT_MSA.3.1 FMT_MSA.3.2
FDP_ACF.1.1 / Signature creation SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / Signature creation SFP FMT_MSA.3.1 FMT_MSA.3.1
FDP_ACF.1.2 / Signature creation SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / Signature creation SFP FMT_MSA.3.1 FMT_MSA.3.0
FDP_ACF.1.3 / Signature creation SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / Signature creation SFP FMT_MSA.3.1 FMT_MSA.3.1
FDP_ACF.1.4 / Signature creation SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / Signature creation SFP FMT_MSA.3.1 FMT_MSA.3.2
FDP_ACF.1.1 / SCD import SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / SCD import SFP FMT_MSA.3.1 FMT_MSA.3.1
FDP_ACF.1.2 / SCD import SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / SCD import SFP FMT_MSA.3.1 FMT_MSA.3.0
FDP_ACF.1.3 / SCD import SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / SCD import SFP FMT_MSA.3.1 FMT_MSA.3.1
FDP_ACF.1.4 / SCD import SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / SCD import SFP FMT_MSA.3.1 FMT_MSA.3.2
FDP_ACF.1.1 / IAS ECC Administration	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / IAS ECC Administration SFP FMT_MSA.3.1 FMT_MSA.3.1

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

SFP		
FDP_ACF.1.2 / IAS ECC Administration SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / IAS ECC Administration SFP FMT_MSA.3.1 FMT_MSA.3.0
FDP_ACF.1.3 / IAS ECC Administration SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / IAS ECC Administration SFP FMT_MSA.3.1 FMT_MSA.3.1
FDP_ACF.1.4 / IAS ECC Administration SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / IAS ECC Administration SFP FMT_MSA.3.1 FMT_MSA.3.2
FDP_ACF.1.1 / Key Management SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / Key Management SFP FMT_MSA.3.1 FMT_MSA.3.1
FDP_ACF.1.2 / Key Management SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / Key Management SFP FMT_MSA.3.1 FMT_MSA.3.0
FDP_ACF.1.3 / Key Management SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / Key Management SFP FMT_MSA.3.1 FMT_MSA.3.1
FDP_ACF.1.4 / Key Management SFP	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	FDP_ACC.1.1 / Key Management SFP FMT_MSA.3.1 FMT_MSA.3.2
FDP_ETC.1.1 / SVD Transfer	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1.1 / SVD Transfer SFP
FDP_ETC.1.2 /	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset	FDP_ACC.1.1 / SVD Transfer SFP

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

SVD Transfer	information flow control]	
FDP_ETC.1.1 / Keys Transfer	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1.1 / Key Management SFP
FDP_ETC.1.2 / Keys Transfer	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1.1 / Key Management SFP
FDP_ITC.1.1 / SCD	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	FDP_ACC.1.1 / SCD Import SFP FMT_MSA.3.1 FMT_MSA.3.2
FDP_ITC.1.2 / SCD	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	FDP_ACC.1.1 / SCD Import SFP FMT_MSA.3.1 FMT_MSA.3.2
FDP_ITC.1.3 / SCD	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	FDP_ACC.1.1 / SCD Import SFP FMT_MSA.3.1 FMT_MSA.3.2
FDP_ITC.1.1 / DTBS	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	FDP_ACC.1.1 / Signature creation SFP FMT_MSA.3.1 FMT_MSA.3.2
FDP_ITC.1.2 / DTBS	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	FDP_ACC.1.1 / Signature creation SFP FMT_MSA.3.1 FMT_MSA.3.2
FDP_ITC.1.3 / DTBS	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1.1 / Signature creation SFP FMT_MSA.3.1

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

	FMT_MSA.3 Static attribute initialisation	FMT_MSA.3.2
FDP_ITC.1.1 / Keys	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	FDP_ACC.1.1 / Key Management SFP FMT_MSA.3.1 FMT_MSA.3.2
FDP_ITC.1.2 / Keys	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	FDP_ACC.1.1 / Key Management SFP FMT_MSA.3.1 FMT_MSA.3.2
FDP_ITC.1.3 / Keys	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	FDP_ACC.1.1 / Key Management SFP FMT_MSA.3.1 FMT_MSA.3.2
FDP_RIP.1.1	N/A	N/A
FDP_SDI.2.1 / Persistent	N/A	N/A
FDP_SDI.2.2 / Persistent	N/A	N/A
FDP_SDI.2.1 / DTBS	N/A	N/A
FDP_SDI.2.2 / DTBS	N/A	N/A
FDP_UCT.1.1 / Receiver	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]	FTP_ITC.1.1 / SCD Import FTP_ITC.1.2 / SCD Import FTP_ITC.1.3 / SCD Import
	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1.1 / SCD Import SFP

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FDP_UIT.1.1 / SVD Transfer	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]	FTP_ITC.1.1 / SVD Transfer FTP_ITC.1.2 / SVD Transfer FTP_ITC.1.3 / SVD Transfer FDP_ACC.1.1 / SVD Transfer SFP
FDP_UIT.1.2 / SVD Transfer	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]	FTP_ITC.1.1 / SVD Transfer FTP_ITC.1.2 / SVD Transfer FTP_ITC.1.3 / SVD Transfer FDP_ACC.1.1 / SVD Transfer SFP
FDP_UIT.1.1 / TOE DTBS	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]	FTP_ITC.1.1 / DTBS import FTP_ITC.1.2 / DTBS import FTP_ITC.1.3 / DTBS import FDP_ACC.1.1 / Signature creation SFP
FDP_UIT.1.2 / TOE DTBS	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]	FTP_ITC.1.1 / DTBS import FTP_ITC.1.2 / DTBS import FTP_ITC.1.3 / DTBS import FDP_ACC.1.1 / Signature creation SFP
FIA_AFL.1.1 / RAD	FIA_UAU.1 Timing of authentication	FIA_UAU 1.1 FIA_UAU 1.2
FIA_AFL.1.2 / RAD	FIA_UAU.1 Timing of authentication	FIA_UAU 1.1 FIA_UAU 1.2
FIA_AFL.1.1 / Authentication keys	FIA_UAU.1 Timing of authentication	FIA_UAU 1.1 FIA_UAU 1.2
FIA_AFL.1.2 / Authentication keys	FIA_UAU.1 Timing of authentication	FIA_UAU 1.1 FIA_UAU 1.2

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FIA_ATD.1.1 / S.Signatory	N/A	N/A
FIA_ATD.1.1 / S.Admin	N/A	N/A
FIA_ATD.1.1 / S.Admin, S.TOE_Admin, S.Personalizer	N/A	N/A
FIA_UAU.1.1	FIA_UID.1 Timing of identification	FIA_UID.1.1 FIA_UID.1.2
FIA_UAU.1.2	FIA_UID.1 Timing of identification	FIA_UID.1.1 FIA_UID.1.2
FIA_UID.1.1	N/A	N/A
FIA_UID.1.2	N/A	N/A
FMT_MOF.1.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1.1 FMT_SMR.1.2 FMT_SMF.1.1
FMT_MSA.1.1 / Administrator – Initialisation	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1.1 / Initialisation SFP FMT_SMR.1.1 FMT_SMR.1.2 FMT_SMF.1.1
FMT_MSA.1.1 / Administrator – Import	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1.1 / SCD Import SFP FMT_SMR.1.1 FMT_SMR.1.2 FMT_SMF.1.1
FMT_MSA.1.1 / Signatory	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of	FDP_ACC.1.1 / Signature creation SFP FMT_SMR.1.1 FMT_SMR.1.2 FMT_SMF.1.1

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

	Management Functions	
FMT_MSA.1.1 / Management of TOE	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1.1 / IAS ECC Administration SFP FMT_SMR.1.1 FMT_SMR.1.2 FMT_SMF.1.1
FMT_MSA.1.1 / Key Management	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1.1 / Key Management SFP FMT_SMR.1.1 FMT_SMR.1.2 FMT_SMF.1.1
FMT_MSA.2.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FDP_ACC.1.1 / Personalisation SFP FDP_ACC.1.1 / IAS ECC Administration SFP FMT_MSA.1.1 / Administrator – Initialisation FMT_MSA.1.1 / Administrator – Import FMT_MSA.1.1 / Signatory FMT_MSA.1.1 / Management of TOE FMT_MSA.1.1 / Key Management FMT_SMR.1.1 FMT_SMR.1.2
FMT_MSA.3.1	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1.1 / Administrator – Initialisation FMT_MSA.1.1 / Administrator – Import FMT_MSA.1.1 / Signatory FMT_MSA.1.1 / Management of TOE FMT_MSA.1.1 / Key Management FMT_SMR.1.1 FMT_SMR.1.2

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FMT_MSA.3.2	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1.1 / Administrator – Initialisation FMT_MSA.1.1 / Administrator – Import FMT_MSA.1.1 / Signatory FMT_MSA.1.1 / Management of TOE FMT_MSA.1.1 / Key Management FMT_SMR.1.1 FMT_SMR.1.2
FMT_MTD.1.1 / Signatory	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1.1 FMT_SMR.1.2 FMT_SMF.1.5
FMT_MTD.1.1 / Admin	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1.1 FMT_SMR.1.2 FMT_SMF.1.4
FMT_MTD.1.1 / Association between SCD and SCD_ID	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1.1 FMT_SMR.1.2 FMT_SMF.1.3
FMT_MTD.1.1 / TOE Serial Number	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1.1 FMT_SMR.1.2 FMT_SMF.1.1
FMT_MTD.1.1 / TOE State	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1.1 FMT_SMR.1.2 FMT_SMF.1.0
FMT_MTD.1.1 / Unblock	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1.1 FMT_SMR.1.2 FMT_SMF.1.1
FMT_SMF.1.1	N/A	N/A
FMT_SMR.1.1	FIA_UID.1 Timing of identification	FIA_UID.1.1
FMT_SMR.1.2	FIA_UID.1 Timing of identification	FIA_UID.1.2
FPT_EMSEC.1.1	N/A	N/A
FPT_EMSEC.1.2	N/A	N/A
FPT_FLS.1.1	N/A	N/A

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FPT_PHP.1.1	N/A	(FMT_MOF.1.1)
FPT_PHP.1.2	N/A	(FMT_MOF.1.1)
FPT_PHP.3.1	N/A	N/A
FPT_TST.1.1	N/A	(FPT_TEE.1)
FPT_TST.1.2	N/A	(FPT_TEE.1)
FPT_TST.1.3	N/A	(FPT_TEE.1)
FTP_ITC.1.1 / SCD Import	N/A	N/A
FTP_ITC.1.2 / SCD Import	N/A	N/A
FTP_ITC.1.3 / SCD Import	N/A	N/A
FTP_ITC.1.1 / SVD Transfer	N/A	N/A
FTP_ITC.1.2 / SVD Transfer	N/A	N/A
FTP_ITC.1.3 / SVD Transfer	N/A	N/A
FTP_ITC.1.1 / DTBS Import	N/A	N/A
FTP_ITC.1.2 / DTBS Import	N/A	N/A
FTP_ITC.1.3 / DTBS Import	N/A	N/A
FTP_TRP.1.1 / TOE	N/A	N/A
FTP_TRP.1.2 / TOE	N/A	N/A

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

FTP_TRP.1.3 / TOE	N/A	N/A

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

6.3.2.2 Justification for not satisfied dependencies

The table bellows provides the justification for the non satisfied dependencies that are identified.

Justification	Missing dependencies	Justification
#1	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	The cryptographic algorithms SHA-1 and SHA-256 do not use any cryptographic key. Therefore none of the listed SFRs are needed to be defined for this specific instantiation of FCS_COP.1.
#2	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Two situation occurs : 1- During the first round of certificate verification, the TOE uses a Root certificate verification public key. When using this key, the following dependencies applies FDP_ITC.1.1 / Keys FDP_ITC.1.2 / Keys FDP_ITC.1.3 / Keys FCS_CKM.4.1 / SCD/SVD As this certificate verification public key may be generated by the TOE, the following dependency applies: FCS_CKM.1.1 / RSA

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

		The certificate contains an ephemeral public key protected by a cryptogram that only the certificate verification public key can check. Upon successful verification of the certificate (ensured by FCS_COP.1.1 / Certificate Verification), the ephemeral public key nested within the certificate is securely imported in the TOE for the next use 2- In next step(s), the certificate is verified with the ephemeral key (which is extracted from a former certificate verification step).The certificate contains a public key protected by a cryptogram that only the certificate verification public key (which is trusted) can check. Upon successful verification of the certificate (ensured by FCS_COP.1.1 / Certificate Verification), the key nested within the certificate (which is an ephemeral key) is securely imported in the TOE for the next use When the certificate verification fails, or when the sequence for certificate verification fails, the ephemeral public key is erased with FDP_RIP.1.1.
#3	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key	The key used for authentication is an ephemeral key. It is securely imported on the TOE through successful certificate verification (ensured by FCS_COP.1.1 / Certificate Verification) and by the initial link of trust coming from the Root Certificate verification public key, whose following dependencies apply :

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

	generation] FCS_CKM.4 Cryptographic key destruction	FDP_ITC.1.1 / Keys FDP_ITC.1.2 / Keys FDP_ITC.1.3 / Keys FCS_CKM.4.1 / SCD/SVD When the User Authentication fails, or when the sequence for authentication is not fulfilled, the ephemeral public key is erased with FDP_RIP.1.1.
#4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	The key used for authentication is an ephemeral key. It is securely imported on the TOE through successful certificate verification (ensured by FCS_COP.1.1 / Certificate Verification) and by the initial link of trust coming from the Root Certificate verification public key, whose following dependencies apply : FDP_ITC.1.1 / Keys FDP_ITC.1.2 / Keys FDP_ITC.1.3 / Keys FCS_CKM.4.1 / SCD/SVD When the Subject authentication fails, or when the sequence for authentication is not fulfilled, the ephemeral public key is erased with FDP_RIP.1.1.

6.3.3 Security Objectives rationale

In the following chapter, all refinements to the OSP, Threats and Assumptions of the [SSCD2] and [SSCD3] are indicated in *blue italic letters*.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

6.3.3.1 Policies and Security Objective Sufficiency

P.CSP_QCert (CSP generates qualified certificates)

establishes the qualified certificate for the signatory and provides that the SVD matches the SCD that is implemented in the SSCD under sole control of this signatory. P.CSP_QCert is addressed by the TOE by **OT.SCD_SVD_Corresp** and **OE.SCD_SVD_Corresp** concerning the correspondence between the SVD and the SCD, in the TOE IT environment, by **OE.CGA_QCert** for generation of qualified certificates by the CGA, respectively.

P.QSign (Qualified electronic signatures)

provides that the TOE and the SCA may be employed to sign data with qualified electronic signatures, as defined by the Directive [1], article 5, paragraph 1. Directive [1], recital (15) refers to SSCDs to ensure the functionality of advanced signatures. The requirement of qualified electronic signatures being based on qualified certificates is addressed by **OE.CGA_QCert**. **OE.SCA_Data_Intend** provides that the SCA presents the DTBS to the signatory and sends the DTBS-representation to the TOE. **OT.Sig_Secure** and **OT.Sigy_SigF** address the generation of advanced signatures by the TOE.

P.Sigy_SSCD (TOE as secure signature-creation device)

establishes the TOE as secure signature-creation device of the signatory with practically unique SCD. This is addressed by **OT.Sigy_SigF** ensuring that the SCD is under sole control of the signatory and **OE.SCD_Unique** and **OT.SCD_Unique** ensuring the cryptographic quality of the SCD/SVD pair for the qualified electronic signature. **OT.Init** provides that generation of the SCD/SVD pair is restricted to authorised users

P.LinkSCD_QualifiedCertificate (Link between a SCD and its qualified certificate)

ensures that the SCA can unambiguously find within the TOE File structure the SCD matching a (qualified) certificate it has chosen to perform an electronic signature. It is addressed by **OE.LinkSCD_QualifiedCertificate** that ensures an unambiguous link between each (qualified) certificate and the matching SCD loaded in the TOE.

P.TOE_PublicAuthKey_Cert (Certificate for asymmetric TOE authentication keys)

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

ensures that each private key(s) of the TOE for authentication matches the public key stored within the relevant certificate issued by an entitled entity. The authentication public key is exported thanks to **OE.TOE_PublicAuthKey_Transfer**.

P.TOE_Construction (TOE construction)

ensures that all the recommendations indicated in [**AGD_PRE**] are applied for the construction of the TOE in phase 6. It is addressed by **OE.TOE_Construction**.

P.eServices (Provision of eServices)

ensures that the TOE provides secure eServices functionalities. It is addressed by **OT.eServices**.

6.3.3.2 Threats and Security Objective Sufficiency

T.Hack_Phys (Exploitation of physical vulnerabilities)

deals with physical attacks exploiting physical vulnerabilities of the TOE. **OT.SCD_Secrecy** preserves the secrecy of the SCD, ***OT.Key_Secrecy*** *preserves the secrecy of all the authentication and eServices keys stored in the TOE*. Physical attacks through the TOE interfaces or observation of TOE emanations are countered by **OT.EMSEC_Design**. **OT.Tamper_ID** and **OT.Tamper_Resistance** counter the threat **T.Hack_Phys** by detecting and by resisting tamper attacks.

T.SCD_Divulg (Storing and copying and releasing of the signature-creation data)

addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in the Directive [1], recital (18). This threat is countered by **OT.SCD_Secrecy** which assures the secrecy of the SCD used for signature generation. **OT.SCD_Transfer** and **OE.SCD_Transfer** ensures the confidentiality of the SCD transferred between SSCDs.

T.SCD_Derive (Derive the signature-creation data)

deals with attacks on the SCD via public known data produced by the TOE. This threat is countered by **OE.SCD_Unique** (in case of SCD import) and **OT.SCD_Unique** (in case of key generation) that provides

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

cryptographic secure generation of the SCD/SVD-pair. **OT.Sig_Secure** ensures cryptographic secure electronic signatures.

T.Sig_Forgery (Forgery of the electronic signature)

deals with non-detectable forgery of the electronic signature. This threat is in general addressed by **OT.Sig_Secure** (Cryptographic security of the electronic signature), **OE.SCA_Data_Intend** (SCA sends representation of data intended to be signed), **OE.CGA_QCert** (Generation of qualified certificates), **OT.SCD_SVD_Corresp** and **OE.SCD_SVD_Corresp** (Correspondence between SVD and SCD), **OT.SVD_Auth_TOE** (TOE ensures authenticity of the SVD), **OE.SVD_Auth_CGA** (CGA proves the authenticity of the SVD), **OT.SCD_Secrecy** and **OT.SCD_Transfer** (Secrecy of the signature-creation data), **OE.SCD_Transfer** (Secure transfer of SCD between SSCD), **OT.EMSEC_Design** (Provide physical emanations security), **OT.Tamper_ID** (Tamper detection), **OT.Tamper_Resistance** (Tamper resistance) and **OT.Lifecycle_Security** (Lifecycle security), as follows: **OT.Sig_Secure** ensures by means of robust encryption techniques that the signed data and the electronic signature are securely linked together. **OE.SCA_Data_Intend** provides that the methods used by the SCA (and therefore by the verifier) for the generation of the DTBS-representation is appropriate for the cryptographic methods employed to generate the electronic signature. The combination of **OE.CGA_QCert**, **OT.SCD_SVD_Corresp**, **OT.SVD_Auth_TOE**, and **OE.SVD_Auth_CGA** provides the integrity and authenticity of the SVD that is used by the signature verification process. **OT.Sig_Secure**, **OT.SCD_Secrecy**, **OT.SCD_Transfer**, **OT.EMSEC_Design**, **OT.Tamper_ID**, **OT.Tamper_Resistance**, and **OT.Lifecycle_Security** ensure the confidentiality of the SCD implemented in the signatory's SSCD and thus prevent forgery of the electronic signature by means of knowledge of the SCD.

T.Sig_Repud (Repudiation of electronic signatures)

deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in his un-revoked certificate. This threat is in general addressed by **OE.CGA_QCert** (Generation of qualified certificates), **OT.SVD_Auth_TOE** (TOE ensures authenticity of the SVD), **OE.SVD_Auth_CGA** (CGA proves the authenticity of the SVD), **OT.SCD_SVD_Corresp** and **OE.SCD_SVD_Corresp** (Correspondence between SVD and SCD), **OT.SCD_Unique** and **OE.SCD_Unique**(Uniqueness of the signature-creation data), **OT.SCD_Transfer** and **OE.SCD_Transfer** (Secure transfer of SCD between SSCD), **OT.SCD_Secrecy** (Secrecy of the signature-creation data), **OT.EMSEC_Design** (Provide physical emanations security), **OT.Tamper_ID** (Tamper detection), **OT.Tamper_Resistance** (Tamper resistance), **OT.Lifecycle_Security** (Lifecycle security), **OT.Sigy_SigF** (Signature generation function for the legitimate signatory only), **OT.Sig_Secure** (Cryptographic security of the electronic signature), **OE.SCA_Data_Intend** (SCA sends representation of data intended to be signed) and **OT.DTBS_Integrity_TOE** (Verification of the DTBS-

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

representation integrity). **OE.CGA_QCert** ensures qualified certificates which allow to identify the signatory and thus to extract the SVD of the signatory. **OE.CGA_QCert**, **OT.SVD_Auth_TOE** and **OE.SVD_Auth_CGA** ensure the integrity of the SVD. **OE.CGA_QCert** and **OT.SCD_SVD_Corresp** ensure that the SVD in the certificate correspond to the SCD that is implemented by the SSCD of the signatory. **OT.SCD_Unique** provides that the signatory's SCD can practically occur just once. **OT.Sig_Secure**, **OT.SCD_Transfer**, **OT.SCD_Secrecy**, **OT.Tamper_ID**, **OT.Tamper_Resistance**, **OT.EMSEC_Design**, and **OT.Lifecycle_Security** ensure the confidentiality of the SCD implemented in the signatory's SSCD. **OT.Sigy_SigF** provides that only the signatory may use the TOE for signature generation. **OT.Sig_Secure** ensures by means of robust cryptographic techniques that valid electronic signatures may only be generated by employing the SCD corresponding to the SVD that is used for signature verification and only for the signed data. **OE.SCA_Data_Intend** and **OT.DTBS_Integrity_TOE** ensure that the TOE generates electronic signatures only for DTBS-representations which the signatory has decided to sign as DTBS.

OT.LifeCycle_Management *ensures that when the TOE is under the Personalisation Agent control, it can not be misused to sign on behalf of the legitimate Signatory.*

OE.LinkSCD_QualifiedCertificate and ***OT.SCD/SVD_Management*** *ensure the SCA always uses the SCD it intends to, in order to create a digital signature.* ***OE.LinkSCD_QualifiedCertificate*** ensures that the SCA can unambiguously sort out within the TOE file structure the SCD matching any (qualified) certificate it has chosen and intends to use. ***OT.SCD/SVD_Management*** *ensures that the TOE create signature with the SCD that has been selected by the SCA. As such it ensures the signature is always created with the SCD matching the (qualified) certificate selected by the SCA, avoiding any mismatch between SCD and (qualified) certificate, that may cause the signature to be repudiated.*

T.SVD_Forgery (Forgery of the signature-verification data)

deals with the forgery of the SVD exported by the TOE to the CGA for the generation of the certificate. **T.SVD_Forgery** is addressed by **OT.SVD_Auth_TOE** which ensures that the TOE sends the SVD in a verifiable form to the CGA, as well as by **OE.SVD_Auth_CGA** which provides verification of SVD authenticity by the CGA.

T.DTBS_Forgery (Forgery of the DTBS-representation)

addresses the threat arising from modifications of the DTBS-representation sent to the TOE for signing which then does not correspond to the DTBS-representation corresponding to the DTBS the signatory intends to sign. The TOE counters this threat by the means of **OT.DTBS_Integrity_TOE** by verifying the integrity of the DTBS-representation. The TOE IT environment addresses **T.DTBS_Forgery** by the means of **OE.SCA_Data_Indent**.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

T.SigF_Misuse (Misuse of the signature-creation function of the TOE)

addresses the threat of misuse of the TOE signature-creation function to create Signed Data Object by others than the signatory to create SDO for data the signatory has not decided to sign, as required by the Directive [1],Annex III, paragraph 1, literal (c). This threat is addressed by the **OT.Sigy_SigF** (Signature generation function for the legitimate signatory only), **OE.SCA_Data_Intend** (Data intended to be signed), **OT.DTBS_Integrity_TOE** (Verification of the DTBS-representation integrity), and **OE.HI_VAD** (Protection of the VAD) as follows: **OT.Sigy_SigF** ensures that the TOE provides the signature-generation function for the legitimate signatory only. **OE.SCA_Data_Intend** ensures that the SCA sends the DTBS-representation only for data the signatory intends to sign. The combination of **OT.DTBS_Integrity_TOE** and **OE.SCA_Data_Intend** counters the misuse of the signature generation function by means of manipulation of the channel between the SCA and the TOE. If the SCA provides the human interface for the user authentication, **OE.HI_VAD** provides confidentiality and integrity of the VAD as needed by the authentication method employed.

OT.LifeCycle_Management *ensures that when the TOE is under the Personalisation Agent control, it can not be misused to sign on behalf of the legitimate Signatory..*

T.Key_Divulg (storing, copying and releasing a key)

addresses the threat against the (1) authentication key of the TOE, (2) the authentication keys of entities and (3) the eServices keys stored in the TOE due to storage and copying of key(s) outside the TOE. This threat is countered by **OT.Key_Secrecy** which assures the secrecy of the keys stored and used by the TOE. **OE.AuthKey_Transfer** ensures the confidentiality of the authentication keys transferred to the TOE.

OT.Key_Lifecycle_Security (Lifecycle security) ensures the secrecy of the keys stored in the TOE during the whole life of the TOE.

T.Key_Derive (Derive a key)

deals with attacks on authentication and eServices keys via public known data produced or received by the TOE (public key, authentication cryptogram,…). This threat is countered by **OE.AuthKey_Unique** (in case of import) and **OT.TOE_AuthKey_Unique** (in case of TOE's authentication key generation) that provides cryptographic secure generation of the keys. **OT.Authentication_Secure** ensures secure authentication cryptograms.

T. +33 (0)1 78 01 70 00 I F. +33 (0)1 78 01 70 20 I Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France I info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

T.TOE_PublicAuthKey_Forgery (Forgery of the public key of a TOE authentication key)

deals with the forgery of the TOE's public key used for authentication exported by the TOE to an entitled entity for the generation of the certificate. This is addressed by **OE.TOE_PublicAuthKey_Transfer** which ensures the authenticity of the TOE's public key for authentication.

T.Authentication_Replay (Replay of an authentication of an external entity)

deals with the threats an attacker retrieves an authentication cryptogram presented to the TOE by an entity and present it again to the TOE is order to grant some rights in order to gain access to some data on the TOE. This is addressed by **OT.Authentication_Secure** that ensures the authentication cryptogram can not be replayed as they rely on random data internally generated by the TOE;

6.3.3.3 Assumption and Security Objective Sufficiency

A.CGA (Trustworthy certification-generation application)

establishes the protection of the authenticity of the signatory's name and the SVD in the qualified certificate by the advanced signature of the CSP by means of the CGA. This is addressed by **OE.CGA_QCert** (Generation of qualified certificates) which ensures the generation of qualified certificates and by **OE.SVD_Auth_CGA** (CGA proves the authenticity of the SVD) which ensures the verification of the integrity of the received SVD and the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

A.SCA (Trustworthy signature-creation application)

establishes the trustworthiness of the SCA according to the generation of DTBS-representation. This is addressed by **OE.SCA_Data_Intend** (Data intended to be signed) which ensures that the SCA generates the DTBS-representation of the data that has been presented to the signatory as DTBS and which the signatory intends to sign in a form which is appropriate for being signed by the TOE

A.SCD_Generate (Trustworthy SCD/SVD generation)

establishes a trustworthy SCD/SVD pair. This that the SCD must be unique, objective met by **OE.SCD_Unique**, that the SCD and the SVD must correspond, objective met by **OE.SCD_SVD_Corresp**.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

The secrecy of the SCD must be maintained while it is transferred to the TOE before being deleted, **OE.SCD_Transfer**.

7 TOE Security Specification

7.1 Description

The TOE inherits all the security functions provided by the underlying javacard open platform [PLT] (see the Security target). On top of these, it adds some supplemental security functions that are described hereafter.

SF.RAD_MGT

This security function is involved in the management of the RAD, whether it is PIN or Biometric based. It ensures the link between each RAD(s) and its associated role (Signatory and Administrator).

It enforces access control over any management operation on the RAD:

- In phase 6, it only allows the RAD(s) to be created by the Personalisation Agent. It requires the RAD to be encrypted in order to ensure its confidentiality. This security function ensures the Personalisation Agent can not verify the RAD, and impersonate the role “Signatory”.
- In phase 7, it only allows the RAD(s) to be created by the administrator. Once loaded, the RAD can only be changed under control of the signatory and unblocked by the Administrator.
- In phase 7, it allows the TOE to authenticate any Role using a RAD comparison (Signatory, and Administrator if it uses a RAD).

This security function manages the validation process of the role associated to the RAD (Signatory or Administrator). It performs the comparison of the VAD with the RAD, and upon successful comparison it authenticates the associated role. Each RAD is associated to an error counter which aims at ensuring its protecting against brute force attacks. Upon each submission of an incorrect VAD, it decrements the error counter, and restores it to its maximum value upon a successful VAD submission. When the error counter has reached ‘00’, the security function blocks the usage of the RAD, and in particular bans the authentication of the associated role, and the ability to change the RAD value (for both the Signatory and the Administrator). Once blocked, the security function allows the unblocking of the RAD after the successful authentication of the role Administrator (please note that the administrator role required to unblock the RAD may be different from the one associated to the blocked RAD if ever).

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d’Estienne d’Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

This security function also ensures secure deallocation of VAD after verification and RAD after update.

This security function allows managing the RAD either through APDU commands, or through shared interfaces (using sharing mechanism). They enable other applets potentially present on the javacard platform to manage the RAD. .The security function ensures the same security policy is applied on both interfaces, so that there are no logical backdoor on the RAD management.

This security function relies on SF.DEV_AUTH and SF.ADM_AUTH to authenticate the role "Administrator" required to create the RAD.

SF.SIG

This security function manages the signature creation service.

It enforces access control over the signature creation service:

- In phase 6, it ensures the signature computation function is not accessible, and in particular that the Personalization Agent can not sign on behalf of the Signatory.
- In phase 7, it ensures the signature creation feature is activated only by the signatory.
- In phase 7, it enforces the DTBS to be sent by an authenticated SCA, in a manner ensuring its integrity, and ensures the role signatory is successfully authenticated before creating the signature.

The security function enables to select the signature key to be used for the signature creation among all the signature key hold by the TOE.

The security function ensures the data hashing (if hash on card, or partial hashing is used), and the secure signature computation using either a RSA or ECDSA private key (SCD). During the signature creation, the coherency with the matching signature public key (SVD) is verified.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

This security function relies on:

- SF.DEV_AUTH to establish a trusted channel with the SCA
- SF.RAD_MGT to authenticate the Signatory
- SF.SM to transmit the DTBS

SF.DEV_AUTH

This security function manages the device authentication between the TOE and an external entity.

The device authentication is a mutual authentication between the TOE and an external entity that may be either realized using symmetric or asymmetric cryptography. Upon successful mutual authentication, the security function computes a shared secret (called the seed) from random numbers generated by both the TOE and the external entity and known only to them. The seed is then used by SF.SM to generate session keys to protect communication in integrity, authenticity and confidentiality, and then maintain the trusted channel. As such, this security function allows generating a trusted channel with an external entity.

This security function allows the mutual authentication with the following external entities:

- Personalisation Agent (phase 6)
- SCA (phase 6 & 7), mingled with the personalisation agent in phase 6
- CGA (phase 6 & 7), mingled with the personalisation agent in phase 6
- SSCD type 1 (phase 6 & 7), mingled with the personalisation agent in phase 6
- IFD (phase 7)

This security function manages as well the validation process of the role associated to the authentication key used by the remote IT entity. Upon successful device authentication, the associated role is authenticated. Each key is associated to an error counter (it may be infinite) which aims at ensuring its protecting against brute force attacks. Upon each wrong authentication, it decrements the error counter (if present), and restores it to its maximum value upon a successful authentication. When the error counter has reached '00', the security function blocks the usage of the key, and bans the authentication of the associated role.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

SF.ADM_AUTH

This security function manages the authentication of external entities by the TOE. It is only active in phase 7.

This security function enables the TOE to authenticate external entities and may be either realized using symmetric or asymmetric cryptography.

This security function manages as well the validation process of the role associated to the authentication key used by the external entity. Upon successful authentication, the associated role is authenticated. Each key is associated to an error counter (it may be infinite) which aims at ensuring its protecting against brute force attacks. Upon each wrong authentication, it decrements the error counter (if present), and restores it to its maximum value upon a successful authentication. When the error counter has reached '00', the security function blocks the usage of the key, and bans the authentication of the associated role.

This security function allows the authentication of the following roles:

- TOE_Administrator
- User_Admin

SF.SM

This security function ensures the protection of communication between the TOE and an external entity. As such, this security function maintains a trusted channel.

This security function requires the TOE and the external entity to establish first a trusted channel using a device authentication (mutual) with SF.DEV_AUTH.

It ensures the following properties:

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

- In phase 6, it maintains the confidentiality, integrity and authenticity of the private keys (including the SCD), the symmetric keys (DES and AES), and the RAD (PIN and biometric template)
- In phase 6, it maintains the integrity and authenticity of the asymmetric public key (including the SVD) when being exported to the outside
- In phase 7, it maintains the confidentiality, integrity and authenticity of communication exchanged between the TOE and the external entity.

In phase 7, the confidentiality, integrity and authenticity of data is ensured by cryptographic means based on symmetric cryptography. Data are encrypted and signed using the symmetric session keys generated from the seed agreed during the device (mutual) authentication (see SF.DEV_AUTH). Moreover, the protection against replay attacks is ensured by the signature which is computed using a dynamic ICV, incremented at each new command.

In phase 6, the confidentiality (for the SCD), integrity and authenticity (for the SVD), is ensured by cryptographic means based on symmetric cryptography. Data are encrypted using the symmetric session keys generated from the seed agreed during the device (mutual) authentication (see SF.DEV_AUTH). The integrity of the SVD is ensured by the

This security function is also in charge of building the session keys from the seed computed by SF.DEV_AUTH. These session keys are ephemeral and unique, as the seed is computed from random numbers generated by the TOE and the external entity.

This security function is also in charge of destroying the session keys in case an error is detected (data not authentic or not integer), or when a command in plan text is sent.

SF.KEY_MGT

This security function is involved in the management of the keys (including SCDs and SVDs).

It enforces access control over any management operation on the keys:

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

- In phase 6, it only allows the key (including the SCD and SVD, and the DH parameters) to be loaded, generated and exported (for the public keys) by the Personalisation Agent. It also requires the private and secret keys to be encrypted in order to ensure their confidentiality. This security function ensures the Personalisation Agent can not use the keys it has loaded or generated. It ensures the personalisation Agent can not impersonate the associated role (in case of authentication keys), or create a signature with the SCD.
- In phase 7, it enforces access control over the management operations on the SCD and SVD (import, generation and export) and ensures the SCD is loaded in an encrypted form to ensure its confidentiality.
- In phase 7, it enforces access control over the management operations on the authentication and eServices keys (import, generation, and export of public keys) and the DH parameters (loading). It ensures that any loading, generation or public export operation is performed by an authenticated entity (Signatory, IFD, SCA, CGA, SSDD type 1, User_Admin), according to the TOE configuration.

This security function also ensures that after update or generation, the key (including SCD and SVD) are securely destroyed.

This security function relies on:

- SF.DEV_AUTH to establish the trusted channel with the SSCD type 1
- SF.RAD_MGT to authenticate the Signatory
- SF.DEV_AUTH and SF.ADM_AUTH to authenticate the roles entitled to perform the operations
- SF.SM to maintain the trusted channel and transmit the DTBS

SF.CONF

This security function manages the configuration of the TOE.

1) It allows the modification of the following TOE attributes in both phase 6 and 7:

- Communication medium : contact and/or contactless
- Type of cryptography to be used for the remote IT entities and remote subject authentication (symmetric or asymmetric)
- Type of DTBS to be used: the DTBS representation fully computed outside the TOE may be used

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

This security function ensures their initialization to a default values when the applet instance is created, and apply an access control over modification. Only the successfully authenticated Personalisation Agent (in phase 6) or “TOE_Administrator” (phase 7) can modify these attributes.

2) It also allows the modification of the following TOE attributes in phase 6:

- TOE serial number
- TOE State

This security function ensures an access control over these operations. Only the successfully authenticated Personalisation Agent can modify these attributes.

3) It also allows the modification in phase 5 of the ability to retrieve the identification data of the TOE. The security function ensures an access control over this operation. Only the successfully authenticated Manufacturing Agent (phase 5) can modify this attributes.

4) It also allows the creation of the container in which the secure data (SCD, SVD, RAD and keys) are stored. The security function ensures an access control over the creation operation. Only the successfully authenticated Personalisation Agent (phase 6) or Administrator (phase 7) can perform this operation.

This security function relies on

- SF.DEV_AUTH to authenticate the role personalisation Agent
- SF.ADM_AUTH to authenticate the role TOE_Administrator

SF.ESERVICE

This security function enables to perform electronic services. It is active in phase 7.

This security function offers the following electronic services:

- C/S authentication

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d’Estienne d’Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

- Decryption key decipherment
- Certificate verification

SF.SAFESTATE_MGT

This security function ensures the TOE is always in a safe state. It monitors the integrity of the TOE, its assets and the TSF data (RAD, keys, DTBS) by performing selftests. When an unexpected event occurs (loss of power, loss of integrity, tearing,…), it ensures

- the TOE returns in a safe state
- all sensitive data are erased
- the TOE returns in a restrictive secure state

When a major issue is detected, the security function ensures the destruction of the TOE, so that the assets are not accessible anymore.

SF.PHYS

This security function ensures the protection of the TOE against physical manipulation aiming at getting access to its assets. In particular, it ensures that the TOE

- detects physical manipulation (I/O manipulation, EM perturbation, temperature perturbation,…) and takes countermeasures.
- is protected against probing and that there is no information leakage that my be used to reconstruct sensitive data

When a major issue is detected, the security function ensures the destruction of the TOE, so that the assets are not accessible anymore.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

8 Annex A : Attributes for FDP_ACF Security attribute based access control

8.1 General Attribute

General Attribute

Subject	Attribute	Status	Remark
User	**Role**	**Administrator**	The role "Administrator" may be granted to several external entities of the TOE. Please refer to §4.2 for more details. The role Admin may be granted upon successful authentication based on a cryptographic mean (authentication) or on a RAD verification (PIN or Biometric comparison). This subject can interact in phase 6 or 7 of the life cycle
		Signatory	The role "Signatory" may be granted upon successful authentication based on a RAD verification (PIN or Biometric comparison) This role can only interact in phase 7 of

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

			the life cycle

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

8.2 Initialisation attribute group

Initialisation attribute group

Subject	Security Attribute	Status	Remark
User	**SCD/SVD Management**	**Authorized**	The TOE controls the access on every object it possess, in particular the SCD and the SVD. In phase 6, the personalisation Agent is the user Admin, and as such always has the attribute "SCD/SVD Management" set to "Authorized". In phase 7, two access mode may be distinguished by the TOE • SCD/SVD generation (SSCD type 3) • SCD/SVD import (SSCD type 2) The access condition is granted to a User if the following conditions are met: • The User is successfully authenticated • The User was given the right to manage the SCD & SVD
		Not authorized	

			(import and/or generation). If theses two conditions are fulfilled, the attribute “SCD/SVD management” is set to “authorized”, otherwise it is set to “not authorized”.

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d’Estienne d’Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

User Data	Security Attribute	Status	Remark
SCD	**Secure SCD Import Allowed**	**No**	The TOE controls the access on every object it possesses, in particular the SCD. In phase 6, the key is imported from a SSCD type 1 that is mingled with the "Personalisation Agent". The security attribute "Secure SCD import" is set to "Yes" when the role "Personalisation Agent" is validated. In phase 7, the access mode SCD Import may be refined to ensure the SCD is imported • from an entitled entity (SSCD type 1) • through a trusted channel ensuring the confidentiality and integrity of the key This refinement does not conflict with SCD/SVD Management
		Yes	The access condition is granted to a remote entities if the following conditions are fulfilled: • The remote entities is successfully authenticated • The remote entities sends the SCD through a secure channel ensuring confidentiality and integrity If theses two conditions are fulfilled, the attribute "Secure SCD Import Allowed" is set to "Yes", otherwise it is set to "No".

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

8.3 Signature creation attribute group

Signature-creation attribute group

User Data	Security Attribute	Status	Remark
SCD	**SCD operational**	**No**	The attribute "SCD operational" is granted by the submission of the RAD by the User Signatory. The RAD may be a PIN or a Biometric template.
		Yes	
DTBS	**Sent by an authorized SCA**	**No**	As the TOE controls the access on every object it possess, it ensures the attribute "Sent by an authorized SCA" for the DTBS is controlled.
		Yes	

8.4 Administration group

Administration group

TOE Attributes	Meaning	Status	Remark
Medium	Communication medium allowed	**Contact**	The TOE may be configured to allow communication in contact and/or contactless mode. The communication to be used by the TOE may be changed in phase 6 by the "Personalisation Agent", and in phase 7 by "TOE_Administrator"
		Contactless	
HashOffCard	Qualified signature computed over hash computed off card	**Authorized**	The TOE may be configured to allow the qualified signature to be computed from a hash off card. It may be changed in phase 6 by the "Personalisation Agent", and in phase 7 by "TOE_Administrator"
		Not authorized	
SymAuthMechanisms	Authentication mechanisms based on symmetric scheme allowed	**Authorized**	The TOE may be configured to enable/disable the authentication mechanism based on symmetric scheme. It may be changed in phase 6 by the
		Not authorized	

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

			"Personalisation Agent", and in phase 7 by "TOE_Administrator"
AsymAuthMechanisms	Authentication mechanisms based on asymmetric scheme allowed	**Authorized**	The TOE may be configured to enable/disable the authentication mechanism based on asymmetric scheme. It may be changed in phase 6 by the "Personalisation Agent", and in phase 7 by "TOE_Administrator"
		Not authorized	

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

8.5 Key Management group

Key Management group

Subject	Security Attribute	Status	Remark
Signatory **User_admin** **SCA** **CGA** **SSCD type 1** **IFD** **Personalisation agent**	**Key import Management**	**Authorized**	In phase 6, the Personalisation Agent has the attribute Key import Management set to Authorized In phase 7, the TOE controls the access on every object it holds, in particular key and Diffie Hellman Domain parameters. The access condition is granted to User, SCA, CGA, SSCD type 1 or IFD if the following conditions are fulfilled: • The Subject is successfully authenticated • The Subject was given the right to import a key (belonging to groups indicated above) When theses two conditions are fulfilled, the attribute Key import management is set to authorized, otherwise it is set to not authorized
		Not authorized	
	Key generation Management	**Authorized**	In phase 6, the Personalisation Agent has the attribute Key generation Management set to Authorized In phase 7, the TOE controls the access on every object it holds, in particular asymmetric key. The access condition is granted to User, SCA, CGA, SSCD type 1 or IFD if the following conditions are fulfilled: • The Subject is successfully authenticated • The Subject was given the right to generate a key (belonging to groups indicated) If theses two conditions are fulfilled, the attribute Key
		Not authorized	

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534

			generation management is set to authorized, otherwise it is set to not authorized
	Key export Management	**Authorized**	In phase 6, the Personalisation Agent has the attribute Key export Management set to Authorized In phase 7, the TOE controls the access on every object it holds, in particular public keys and Diffie Hellman Domain parameters
		Not authorized	The access condition is granted to User, SCA, CGA, SSCD type 1 or IFD if the following conditions are fulfilled: • The Subject is successfully authenticated • The Subject was given the right to export a key (belonging to groups indicated) If theses two conditions are fulfilled, the attribute Key export management is set to authorized, otherwise it is set to not authorized

T. +33 (0)1 78 01 70 00 | F. +33 (0)1 78 01 70 20 | Oberthur Technologies - 420, rue d'Estienne d'Orves - 92700 Colombes - France | info@oberthur.com
S.A. AU CAPITAL de 22 310 409,20€ - RCS NANTERRE 340 709 534